Audit Protocols

Appendix A

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.1 Management and staff shall receive security training, security awareness, and have security expertise.						
1.1.1 Security training includes: (1) awareness training; (2) periodic security reminders; (3) user education concerning virus protection; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).	1. Review training syllabus for inclusion of the required training. 2. Review a sample of training records to confirm completion of the required training. 3. Review documented procedure for generation of security reminders. 4. Interview a sample of site personnel to verify that documented training was received.	☐	☐	☐ ____	☐ ____	☐
1.1.2 Security skill needs are accurately identified and included in job descriptions and HCFA Business Partners meet these requirements.	1. Review the job descriptions for identification of security skills required. 2. Evaluate the apparent relevance of the specified security skills to the job described.	☐	☐	☐ ____	☐ ____	☐
1.1.3 All Medicare employees and contractor personnel are provided security awareness training prior to being allowed access to Federal tax returns and return information (FTI) or Medicare data, and then are provided annual security refresher training. The training is customized based on job responsibilities.	1. Review training syllabus for inclusion of security awareness training. 2. Review policies and procedures for inclusion of the required process. 3. For a sample of personnel having access to FTI, review personnel records for documentation of receipt of security awareness training. 4. For a sample of personnel having access to FTI, review training documentation and job descriptions for apparent customization of security awareness training to job responsibilities. 5. Interview a sample of personnel having access to FTI to determine if they are aware of their responsibilities relating to handling of FTI.	☐	☐	☐ ____	☐ ____	☐
1.1.4 Security training is adjusted to the level of the employee's responsibilities.	For a sample of personnel, review training documentation and job descriptions for apparent customization of security training to the level of job responsibilities.	☐	☐	☐ ____	☐ ____	☐
1.1.5 The employees acknowledge, in writing, having received the security and awareness training.	Verify that records show all employees have acknowledged receiving security and awareness training.	☐	☐	☐ ____	☐ ____	☐
1.1.6 A record of the security awareness training subject(s) covered is maintained.	1. Verify that the records being maintained allow identification of the security training subjects that have been presented to each employee. 2. Verify that records are being maintained that document the security training subjects covered.	☐	☐	☐ ____	☐ ____	☐
1.1.7 Employees are trained so that they are aware of the restrictions against unauthorized activities and accesses, including the illegal copying of data or software.	1. For a sample of employees, interview to confirm that they are aware of the restrictions against unauthorized activities and accesses, including the illegal copying of data or software. 2. For a sample of employees, review training records and related training syllabuses to confirm training on restrictions against unauthorized activities and accesses, including the illegal copying of data or software.	☐	☐	☐ ____	☐ ____	☐
1.1.8 Training in emergency procedures is conducted at least once a year.	Review a sample of training records and the related syllabus to confirm that training in emergency procedures has been conducted at least annually.	☐	☐	☐ ____	☐ ____	☐
1.1.9 Policy and training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided.	Review documentation of policy and training to confirm the protection of copyright information under the terms of the provision of the copyright holder.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.2 Management shall ensure that corrective security actions are effectively implemented.						
1.2.1 Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.	1. Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested. 2. Review logs and policy documentation to verify that security corrective actions have been monitored on a continuing basis.	☐	☐	☐	____ ☐	____ ☐
1.3 Handling, storage, and destruction of Federal tax returns and return information (FTI) shall be formally controlled.						
1.3.1 Agencies transmitting (FTI) from a main frame computer to another computer, need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission.	1. Review disclosure list for entries indicating that the documented process has been followed. 2. Interview responsible individual(s) to confirm understanding of the required procedure. 3. Review relevant policies and procedures for inclusion of the required logging process elements. 4. For a sample of documents being received from the IRS, observe handling of receipt of FTI for compliance with established procedures.	☐	☐	☐	____ ☐	____ ☐
1.3.2 A listing of all documents received from the IRS is maintained by: (1) taxpayer name; (2) tax year(s); (3) type of information (e.g., revenue agent reports, Form 1041, work papers, etc.); (4) reason for the request; (5) date requested; (6) date received; (7) exact location of the FTI; (8) who has had access to the data; and (9) if disposed of, date and method of disposition.	1. For a sample of documents received, confirm that locations or dispositions are correctly logged, and that all required information is being maintained. 2. Review disclosure list for entries indicating that the documented process has been followed for access to FTI. 3. Observe handling of receipt of FTI from the IRS for compliance with established procedures. 4. Interview responsible individual(s) to confirm understanding of the required procedure. 5. Review relevant policies and procedures for inclusion of the required document handling process elements.	☐	☐	☐	____ ☐	____ ☐
1.3.3 FTI information, other than that on magnetic tape files, disclosed outside the HCFA Business Partner's system is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.	1. Observe transmittal of FTI for compliance with established procedures. 2. Review relevant policies and procedures for inclusion of the required logging process elements. 3. Review disclosure list for entries indicating that the documented process has been followed. 4. Interview responsible individual(s) to confirm understanding of the required procedure.	☐	☐	☐	____ ☐	____ ☐
1.3.4 Appropriate controls are established for all sensitive data entering or leaving the facility. A system is employed that precludes erroneous or unauthorized transfer of data, regardless of media or format. Include controls that maintain a record for the logging of shipping and receipts and a periodic reconciliation of these records.	1. Evaluate the identified control procedures for inclusions of maintenance of records logging all shipping and receipts, and of periodic reconciliation of these records. 2. Review documented procedures for control of sensitive data entering or leaving the facility. 3. Evaluate the identified control procedures for inclusions of specific protections against erroneous or unauthorized transfers.	☐	☐	☐	____ ☐	____ ☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.3.5 A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.	1. Review the documented procedure for destruction of data. 2. Verify that the reviewed procedure includes protections against sensitive data becoming available to unauthorized personnel.	☐	☐	☐	☐	☐
1.3.6 All retired, discarded, or unneeded sensitive data is disposed in a manner that prevents unauthorized persons from using it. All sensitive data is erased from storage media before releasing as work tapes, disks or memory areas. Ensure the destruction of any FTI or sensitive hard copy documents when no longer needed.	1. Review disposal procedures for inclusion of use of approved destruction methods during disposal of hard copy documents that are no longer needed. 2. For a sample of employees, interview to determine that disposal procedures are known and being followed. 3. Review disposal procedures for inclusion of use of approved sanitization procedures before release of any nonvolatile storage devices or media. 4. Review disposal procedures for inclusion of protections against use of retired, discarded, or unneeded sensitive data by unauthorized persons.	☐	☐	☐	☐	☐
1.3.7 Sensitive data and HCFA Business Partner records (Part A and Part B claims and benefit check records) are stored on-site. When on-site storage is not available, commercial storage facilities are used that most closely meet Federal standards for agency records centers. (Obtain Federal standards on National Archives Record Administration [36 CFR part 1228 subpart K]).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. By inspection confirm that the specified data and records are stored on-site.	☐	☐	☐	☐	☐
1.3.8 FTI is never disclosed to agents/contractors during disposal unless authorized by the Internal Revenue Code (IRC). Destruction of FTI is witnessed by an agency employee. However, an agency may elect to have the destruction certified by the contractor in the absence of agency participation.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review a sample of destruction records to confirm consistent use of the procedure.	☐	☐	☐	☐	☐
1.3.9 Before releasing files to an individual or agency or contractor not authorized access to FTI, care is taken to remove all such FTI data, magnetic media will be degaussed after removal.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming consistent use of the required procedure.	☐	☐	☐	☐	☐
1.3.10 FTI is physically destroyed by authorized personnel, or returned to the IRS, or to the system security administrator.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming consistent use of the required procedure.	☐	☐	☐	☐	☐
1.3.11 Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. When FTI information is returned to HCFA a receipt process is used.	1. Confirm by inspection that facility has latest version of IRS Publication 1075. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming consistent use of the required receipt process.	☐	☐	☐	☐	☐
1.3.12 Destruction methods are as follows: (1) burning - the material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (2) mulching or pulping - all material is reduced to particles one inch or smaller; (3) shredding or disintegrating - paper is shredded to effect 5/16 inch wide or smaller strips, and microfilm is shredded to 1/35 - inch by 3/8 - inch strips.	1. Review documentation confirming that destruction is accomplished using one or more of the approved methods. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.3.13 Procedures are implemented to clear sensitive data and software from discarded and transferred equipment and media.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of recently discarded or transferred items, review documentation confirming clearing of data and software in accordance with the procedures.	☐	☐	☐ ____	☐ _____	☐
1.3.14 Inventory records of magnetic media containing FTI are maintained for purposes of control and accountability. Hardcopy printout of a tape or file is recorded in a log that identifies the contents, date received, number of records, and the reel/cartridge control number. If disposed of, the date and method of disposal is recorded. All deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming consistent use of the required procedure.	☐	☐	☐ ____	☐ _____	☐
1.3.15 Semiannual inventories of removable storage devices and media are performed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of the required inventories to confirm that they are being performed at least semiannually.	☐	☐	☐ ____	☐ _____	☐
1.3.16 Removable storage devices and media containing FTI are secured before, during, and after processing, and a proper acknowledgement form is signed, and returned to the IRS.	1. Review audit data confirming consistent use of the required procedure. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ _____	☐
1.3.17 Whenever possible computer operations are in a secure area with restricted access. FTI is kept locked when not in use. Tape reels, disks, or other magnetic media are labeled as Federal Tax Information. Magnetic media is kept in a secure area.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming location of computer operations are in a secure area with restricted access, or that establishes approved use of equivalent safeguards.	☐	☐	☐ ____	☐ _____	☐
1.4 Owners and users shall be aware of security policies.						
1.4.1 Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; and (6) assuring that system users, including maintenance personnel, receive security awareness training.	1. Review a sample of training records to confirm completion of security awareness training. 2. Review training syllabus for inclusion of the security awareness training. 3. Review relevant policies and procedures for inclusion of the prescribed features. 4. Review personnel security records and job descriptions to verify that operating and maintenance personnel have the proper clearances. 5. Review access and maintenance logs, and interview a sample of operating and maintenance personnel, to verify that all maintenance access is logged, and that all maintenance is performed or supervised by authorized, knowledgeable personnel.	☐	☐	☐ ____	☐ _____	☐
1.4.2 To provide reasonable assurance that FTI is adequately safeguarded, an annual self assessment is conducted which addresses the safeguard requirements imposed by the IRS. A copy of the self assessment is submitted to HCFA.	1. Review relevant policies and procedures for inclusion of the required self assessment process. 2. Review documentation confirming submittal of the most recent self assessment to HCFA.	☐	☐	☐ ____	☐ _____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.4.3 Reporting Improper Inspections or Disclosures of FTI - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor who contacts HCFA for submission to the appropriate regional office of the Treasury Inspector General for Tax Administration.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm familiarity with the policy and how to report such improper activity.	☐	☐	☐ ____	☐ ____	☐
1.4.4 Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; and (3) rules that describe expected behavior of all with access to the system.	1. Review policies and procedures for the required distribution process(es). 2. Review the distributed security policies for inclusion of the required rules.	☐	☐	☐ ____	☐ ____	☐
1.4.5 Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. The procedures: (1) stipulate what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.	Review relevant policies and procedures for inclusion and directed use of the required procedures.	☐	☐	☐ ____	☐ ____	☐
1.4.6 Medicare information is not used in the contractor's private line of business unless authorized by HCFA as consistent with the Privacy Act.	1. Review relevant policies for inclusion of this directive. 2. For a sample of employees, interview to confirm awareness of, and adherence to this policy.	☐	☐	☐ ____	☐ ____	☐
1.4.7 Employees are discouraged from browsing sensitive data files by making it clear that company policy prohibits it.	1. Interview a sample of employees to confirm awareness of, and adherence to this policy. 2. Review relevant policies for inclusion of the required directive.	☐	☐	☐ ____	☐ ____	☐
1.4.8 Operating procedures, systems specifications, record layouts, and other documentation are distributed on a "need-to-know" basis.	1. Review relevant policies and procedures for inclusion of the required controls. 2. Review audit data supporting application of the required control to distribution of these documents.	☐	☐	☐ ____	☐ ____	☐
1.5 Information security responsibilities shall be clearly assigned.						
1.5.1 The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3)) senior management; and (4) security administrators.	1. Review the security plan for inclusion of the required identification of ownership of each computer-related resource, and of responsibilities for managing access to each of these resources. 2. Review the security plan for inclusion of definition of security responsibilities and expected behavior for at least each of the four specified categories of personnel.	☐	☐	☐ ____	☐ ____	☐
1.5.2 The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.	Review documentation verifying that an SSO with the required qualifications is designated at an overall level, and at any subordinate levels designated as appropriate by the Business Partner.	☐	☐	☐ ____	☐ ____	☐
1.5.3 If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	1. If these additional SSO positions exist, review documentation supporting use of the specified process. 2. If these additional SSO positions exist, review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.5.4 The SSO is organizationally independent of IS operations.	Review documentation supporting the required organizational independence.	☐	☐	☐	☐	☐
1.5.5 The SSO assures compliance with HCFA's systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with HCFA systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by HCFA Regional Officer and/or Consortium; (4) ensuring that internal controls are incorporated into new ADP information systems; (5) ensuring that systems security requirements are included in RFPs and subcontracts involving Medicare claims processing; (6) maintaining systems security documentation for review by HCFA Regional Officer and/or Consortium; (7) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; and (8) keeping up with new/advanced systems security technology; (9) is a member of all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (10) makes certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.	1. Review documentation supporting SSO performance of each of the specified roles and responsibilities. 2. Review relevant policies and procedures for inclusion of the required SSO roles and responsibilities.	☐	☐	☐	☐	☐
1.5.6 The SSO in each HCFA Business Partner organization is responsible for assisting Application System Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.	1. Review relevant documentation for designation of this security officer. 2. Review relevant policies and procedures for inclusion of identification of the specified roles and responsibilities of this security officer.	☐	☐	☐	☐	☐
1.5.7 Documentation designates specific employees responsible for securing removable storage devices and media.	Review documentation supporting designation of this responsibility to specific employees.	☐	☐	☐	☐	☐
1.6 Records of disclosures to Auditors shall be maintained.						
1.6.1 When auditors read large volumes of records containing FTI, whether in paper or digital format, they need only identify the bulk records examined. This identification contains: (1) approximate number of taxpayer records; (2) dates of the inspection; (3) description of the records; and (4) name of the individuals making the inspection.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting use of the required records process. 3. Interview responsible individual(s) to confirm understanding of the required procedure.	☐	☐	☐	☐	☐
1.7 An incident response capability shall be implemented.						
1.7.1 Procedures exist to identify and report incidents: (1) security incident procedures; (2) report procedures; and (3) response procedures.	1. Review the security incident handling procedure for inclusion of processes for incident reporting and incident response. 2. Review security incident procedures	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.7.2 The HCFA Business Partner's incident response capability has the following characteristics: (1) an understanding of the HCFA Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; and (5) links to other relevant groups.	Review documentation supporting existence of the required characteristics within the Business Partner's incident response capability.	☐	☐	☐ ____	☐ ____	☐
1.8 FTI data to be protected shall be divided into Security levels as appropriate.						
1.8.1 FTI is considered to be at the High sensitivity level and is to be protected as indicated in section 4 of the IRS 1075.	Examine the security plan to verify that the combinations of protection implemented match those specified in the Protective Alternative Chart, IRS 1075.	☐	☐	☐ ____	☐ ____	☐
1.9 Minimum protection standards shall consider local factors.						
1.9.1 Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.	Review relevant policies and procedures for inclusion of the required security management features.	☐	☐	☐ ____	☐ ____	☐
1.9.2 Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the system security plan.)	Confirm by inspection that the required documentation is on file.	☐	☐	☐ ____	☐ ____	☐
1.9.3 The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	1. Review risk assessment policy for inclusion of the required factors. 2. Review the most recent high-level risk assessment for documentation of consideration of the required factors.	☐	☐	☐ ____	☐ ____	☐
1.9.4 A risk assessment is conducted whenever significant modifications are made to a system, facility, and network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (Disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (Policy, procedure, separating duties, training, posters/notices/ announcements, testing/validating/editing, audit routines, audit trails/logs, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).	1. Review relevant policies and procedures for inclusion and directed use of the required process for determining the need for reassessment. 2. Review relevant policies and procedures for inclusion and directed use of the required content. 3. Review the most recent risk assessment for documented inclusion of the required content.	☐	☐	☐ ____	☐ ____	☐
1.9.5 Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	1. Review documentation supporting an assessment that all facilities housing sensitive and critical resources have been identified. 2. Review documentation supporting an assessment that all significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.9.6 Major applications undergo independent review or audit at least every three years.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying conduct of an independent review or audit at least every three years.	☐	☐	☐ ____	☐ ____	☐
1.9.7 All files are reviewed once a year to assure that no data is being collected or maintained that is not currently authorized in the Federal Register.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming execution of the review process at least once a year.	☐	☐	☐ ____	☐ ____	☐
1.9.8 A compliance review or self assessment is conducted once a year.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming execution of the review process at least once a year.	☐	☐	☐ ____	☐ ____	☐
1.9.9 Top management initiates prompt actions to correct deficiencies.	1. Review documentation supporting consistent prompt action by top management to correct deficiencies. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
1.9.10 Major systems and applications are approved by the managers whose missions they support.	1. Inspect documentation of approval for each major system and application by the specified manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
1.9.11 Local Information System risk factors are assessed in accordance with NIST 800-12 Chapter 7.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation verifying assessment of local risk factors in accordance with the reference.	☐	☐	☐ ____	☐ ____	☐
1.9.12 Management analyzes local circumstances to determine space, container, and other security needs at individual facilities that may exceed the Minimum Protection Standards (Table in 4.1 of IRS 1075).	Review documentation establishing that a location-specific Risk Analysis was conducted in development of each applicable System Security Plan.	☐	☐	☐ ____	☐ ____	☐
1.10 A System Security Plan (SSP) shall be documented, maintained, approved, and annually reviewed.						
1.10.1 The following are available and accomplished: (1) security configuration management documentation; (2) hardware/software installation and maintenance review and testing for security features; (3) inventory records; (4) security testing; and (5) virus checking.	1. Review the security plan for inclusion of the required elements 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation supporting completion of the required security testing.	☐	☐	☐ ____	☐ ____	☐
1.10.2 Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.10.3 A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties and covers the topics prescribed by OMB Circular A-130 such as:(a) Rules of the system/Application rules; (b) Training/Specialized training; (c) Personnel controls/Personnel security; (d) Incident response capability; (e) Continuity of support/Contingency planning; (f) Technical security/Technical controls; (g) System interconnection/Information sharing; (h) Public access controls.	1. Review documentation verifying that a security plan covers all major facilities and operations. 2. Review documentation verifying that the security plan has been approved by all key affected parties. 3. Inspect the security plan to confirm that it covers all of the specified topics.	☐	☐	☐ ____	☐ ____	☐
1.10.4 A system security plan has been prepared, in accordance with the HCFA SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).	1. Review documentation establishing that preparation of the plan was in accordance with the HCFA SSP Methodology. 2. Review documentation verifying coverage by system security plans for all applications categorized as MA and GSS.	☐	☐	☐ ____	☐ ____	☐
1.10.5 The Contractor System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, HCFA, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit trails, logs and visitor sign-in sheets.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Verify by inspection that the Contractor Security Profile is maintained and contains the eleven required elements.	☐	☐	☐ ____	☐ ____	☐
1.10.6 Retention procedures are established for all sensitive Medicare data and FTI data.	Review documents establishing the appropriate retention procedures.	☐	☐	☐ ____	☐ ____	☐
1.10.7 Documentation is available to assure that the level of sensitivity and criticality designations of each system has been assigned and has been determined to be commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	Review documentation establishing that the required designations have been assigned with the considerations specified.	☐	☐	☐ ____	☐ ____	☐
1.10.8 Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data verifying that vulnerability identification has been performed as specified. 3. Establish by inspection that the required summary lists are available.	☐	☐	☐ ____	☐ ____	☐
1.10.9 The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting conduct of the required periodic reviews. 3. Review audit data supporting periodic reconsideration of current conditions and risks, and adjustments to the plan as appropriate.	☐	☐	☐ ____	☐ ____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.10.10 The system security plan establishes a security management structure with adequate independence, authority and expertise.	1. Verify by inspection that the system security plan contains the required management structure. 2. Review documentation supporting the assertion that the security management structure meets the stated requirements.	☐	☐	☐	☐	☐
1.11 Security policies shall exist that address hiring, transfer, termination, and performance.						
1.11.1 For prospective employees, references are contacted and background checks performed.	1. Inspect personnel records to confirm that references have been contacted and background checks have been performed. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
1.11.2 Regular job or shift rotations are required.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review staff assignment records to confirm that job and shift rotations occur.	☐	☐	☐	☐	☐
1.11.3 Regularly scheduled vacations exceeding several days are required.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of personnel records to confirm compliance with the required vacation policy.	☐	☐	☐	☐	☐
1.11.4 Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.	1. Review termination and transfer procedures for inclusion of the required processes. 2. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist. 3. For a selection of terminated or transferred employees, examine documentation showing compliance with policies.	☐	☐	☐	☐	☐
1.11.5 Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.	1. Review documentation establishing that reinvestigation policies for each position are consistent with the specified criteria. 2. Inspect personnel records to confirm sensitive position have had background reinvestigations performed within the required period.	☐	☐	☐	☐	☐
1.11.6 Confidentiality or security agreements are required for employees and contractors assigned to work with confidential information.	1. Review policies on confidentiality or security agreements. 2. Determine whether confidentiality or security agreements are on file.	☐	☐	☐	☐	☐
1.12 Disclosure of FTI by HCFA Business Partners to their subcontractors shall be controlled.						
1.12.1 Disclosure of FTI is generally prohibited.	1. Review Authorized Disclosure Agreements. 2. Review relevant policies for inclusion and directed use of the required directive.	☐	☐	☐	☐	☐
1.13 Descriptions of Medicare operations, records, and assets are validated once a year.						
1.13.1 The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package.	Inspect the SSP and certification package for the required signatures.	☐	☐	☐	☐	☐
1.13.2 The safeguard selection decisions and the risk assessment reports submitted are carefully reviewed.	Examine documentation supporting completion of the required review.	☐	☐	☐	☐	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
1. *Entitywide Security Program Planning and Management*						
1.13.3 The HCFA Business Partner is responsible for approving any necessary corrective action plans.	1. Review audit data supporting compliance with the required approval process. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. A plan of action is documented for correction informaition security dificancies.	☐	☐	☐ ____	☐ ____	☐
1.13.4 The HCFA Business Partner's systems security certification is completed annually and is fully documented.	1. Review documentation confirming that the last HCFA Business Partner's systems security certification or recertification was completed within the last year. 2. Review documentation supporting an assertion that the security system is fully documented. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
1.13.5 Formal chain of trust partner agreements (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged) are in place to cover all electronically exchanged data between the contractor and other partners.	Review documentation supporting the assertion that all required formal chain of trust partner agreements are in place.	☐	☐	☐ ____	☐ ____	☐
1.14 General workstation security requirements shall be established.						
1.14.1 Policy/Guideline on workstation use is available.	1. Verify by inspection that the required policy/guideline is available. 2. Interview a sample to confirm familiarity with the required document.	☐	☐	☐ ____	☐ ____	☐
1.14.2 Policy states that employees are not permitted to bring their personally owned computers into the workplace.	Review the specified policy.	☐	☐	☐ ____	☐ ____	☐
1.14.3 All HCFA-owned software is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.	1. Interview programmers and system manager. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review audit data confirming enforcement of the required process.	☐	☐	☐ ____	☐ ____	☐
1.14.4 Only C2 level Network Operating System (NOS) configurations are utilized. See IRS 1075, Sections 5.6 and 5.7, and Exhibit 6.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that all network operating systems are rated C2 level in the configurations used.	☐	☐	☐ ____	☐ ____	☐
1.14.5 If HCFA Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the process used to assure compliance with the required policy.	☐	☐	☐ ____	☐ ____	☐
1.14.6 Policies will be established for controlling the use of laptops, notebooks and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.	Determine the effectiveness of controlling portable terminals by review business partner moble computing policies.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.1 Audit trails shall be maintained.						
2.1.1 User account activity audits are conducted using automated audit controls.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing the automated controls installed to implement the required process. 3. Inspect activity audit logs to confirm continuing use of the required process.	☐	☐	☐ ____	☐ _____	☐
2.1.2 Computers systems processing FTI are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing FTI is accountable.	1. Review documentation identifying all security features of each hardware and software item in the system, and the extent to which each feature is available and activated. 2. Review documentation establishing that the computer systems processing FTI are secured from unauthorized access. 3. For a sample of hardware and software security features, obtain demonstrations of feature operation. 4. Review documentation describing how audit facilities are utilized to assure that everyone accessing a computer system containing FTI is accountable.	☐	☐	☐ ____	☐ _____	☐
2.1.3 All activity involving access to and modifications of sensitive or critical files is logged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing how compliance with this requirement is assured. This should include documentation specifically designating all files considered sensitive or critical, with identification of the corresponding logging methodology for each of these files. 3. Inspect samples of the specified audit logs to confirm continuing use of the required process.	☐	☐	☐ ____	☐ _____	☐
2.1.4 Access to audit logs is restricted.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required restrictions. 3. Review security software settings and compare with system security policies and procedures. 4. Inspect a sample of audit log access lists.	☐	☐	☐ ____	☐ _____	☐
2.1.5 The audit trail includes sufficient information to establish what events occurred and who or what caused them.	1. Review a sample of event logs and audit records to confirm the required content. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ _____	☐
2.1.6 Every data update written to a file is logged. The record is annotated to show what was changed, when it was changed and by whom.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of the required data update audit logs to confirm that they contain the required information.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.1.7 Audit logs are reviewed periodically and retained for the same period as the original claim.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that audit logs are being retained for the same period as the related claim. 3. Inspect a sample of audit data confirming that the required reviews have been conducted.	☐	☐	☐	☐	☐
2.1.8 All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.	1. Inspect device configurations to confirm that all detected errors that can be logged are being logged. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Determine that audit logs have sufficient detail to assist with fault isolation and resolution of security abnormalities.	☐	☐	☐	☐	☐
2.2 Adequate physical security controls shall be implemented: (1) physical safeguards shall be established that are commensurate with the risks of physical damage or access; (2) visitors shall be controlled.						
2.2.1 Physical Intrusion Detection Systems (IDS) are used for FTI in conjunction with other measures to provide forced entry protection for after-hours security. Alarms annunciate at an on-site protection console, a central station, or local police station. IDS include, but are not limited to: (1) door and window contacts; (2) magnetic switches; (3) motion detectors; and (4) sound detectors.	1. Review physical intrusion detection policies and procedures for spaces and rooms containing FTI for inclusion of the specified approach. 2. Review documentation describing measures used in conjunction with IDS to enhance protections provided directly by the IDS.	☐	☐	☐	☐	☐
2.2.2 FTI (including tapes or cartridges) are placed in secure storage in a secure location, safe from unauthorized access. All containers, room, buildings, and facilities containing FTI are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	1. Review facility security plan for procedures and policies for protection of FTI. 2. Inspect to confirm the use of the documented locking systems and other security measures for physical protection of FTI data.	☐	☐	☐	☐	☐
2.2.3 Locking Systems for Secured Areas and Security Rooms - High Security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders are to have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master". Convenience type locking devices (card keys, sequence button activated locks, etc.) are authorized for use only during duty hours. Keys to secured areas are not in personal custody of an unauthorized employee and any combinations are stored in a security container.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of locks and locking mechanisms for inclusion of the specified features.	☐	☐	☐	☐	☐
2.2.4 Restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. The main entrance to restricted areas is controlled/manned. Lesser entrances have cameras or electronic intrusion detection devices, such as card keys to monitor access.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the required controls. 3. Inspect restricted area access points to confirm that the documented controls are in place and operational.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.2.5 Locked Containers include the following features: (1) commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with locking drawers; and (2) locks must have built in key or hasp and lock.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of containers to confirm inclusion of the required features.	☐	☐	☐ ____	☐ _____	☐
2.2.6 Visitors to sensitive areas, such as the main computer room, tape/media library, and Restricted Areas within the definition of IRS 1075, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a Restricted Area, the identity of visitors is verified, and a new Authorized Access List (AAL) is issued monthly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of sign-in/sign-out registers to confirm collection of the required information. 3. Review a sample of audit data confirming compliance with the required register close out and review actions 4. Inspect a sample of audit data confirming monthly issue of a new AAL.	☐	☐	☐ ____	☐ _____	☐
2.2.7 Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, or other evacuation procedures.	1. Review written emergency procedures for inclusion of the required process. 2. Inspect a sample of audit data confirming use of the required process.	☐	☐	☐ ____	☐ _____	☐
2.2.8 Transmission and Storage Data - FTI may be stored on hard disk only if HCFA Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documentation of approval and installation of the required devices. 3. Review documentation confirming that the access control devices include the required features. 4. Review audit data confirming accomplishment of the required maintenance and upgrades, 5. Review audit data confirming consistent use of the required control devices.	☐	☐	☐ ____	☐ _____	☐
2.2.9 Unissued keys or other entry devices are secured.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of unissued entry devices to confirm that they are secured in accordance with the documented process.	☐	☐	☐ ____	☐ _____	☐
2.2.10 Sensitive information is stored in security containers that have one of the following devices: (1) metal lateral key lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull drawer cabinets with center or off-center lock bars secured by security padlocks; and (4) key lock "mini safes" properly mounted with appropriate key control.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of security containers used for storage of sensitive information to confirm that they comply with the requirements. 3. Review documentation supporting the contention that the required process is followed for storage of sensitive information.	☐	☐	☐ ____	☐ _____	☐
2.2.11 If safes and/or vaults are used, they comply with: (1) safe - GSA approved container of Class I, IV and V and Underwriters Laboratories (UL) listing of TRTL-30, TXTL-60 and TRTL-60; and (2) vaults - hardened room that uses UL approved vault doors and meet GSA specifications.	Examine safe(s) or vault(s) for accompanying manufacturer documentation.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.2.12 Handling and Transporting FTI - Care is taken to safeguard FTI information at all times. If hand carried, it is kept with an individual and protected from unauthorized disclosure. All shipments are documented on transmittal forms and monitored. All FTI transported through the mail or courier/messenger service is double sealed. FTI is clearly labeled "Federal Tax Information".	1. Review FTI handling and transporting policies and procedures for control technique compliance. 2. Review FTI transmittal forms for accuracy and completeness. 3. Inspect a sample of FTI data media for labeling compliance with the requirement.	☐	☐	☐ ____	☐ ____	☐
2.2.13 Security Rooms include the following features: (1) room is enclosed by slab-to-slab walls constructed of approved materials; (2) unless electronic intrusion detection devices are used, all doors entering the space are locked and strict key or combination control should be exercised; (3) door hinge pins must be non-removable or installed on the inside of the room; (4) any glass in doors or walls are security glass (a minimum of two layers of 1/8 inch plate glass with .006 [1/32] vinyl interlayer, normal thickness is 5/26 inch); (5) plastic glazing material is not acceptable; and (6) Vents or louvers are protected by Underwriters' Laboratory (UL) approved electronic detection system that will annunciate at a protection console.	If Security Rooms are used, review documentation confirming that each includes all of the required features.	☐	☐	☐ ____	☐ ____	☐
2.2.14 FTI is locked in cabinets or sealed in packing cartons while in transit. IRS material remains in the custody of an IRS or HCFA or HCFA Business Partner employee. Accountability is maintained during the move.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data supporting continuing use of the required processes.	☐	☐	☐ ____	☐ ____	☐
2.2.15 Key combinations are changed when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.	1. Review audit data confirming consistent use of the required process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.2.16 All entry code combinations are changed periodically.	1. Review documentation and logs for entry code changes. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.2.17 Workstation locations are secured.	Review documentation confirming that all workstations are in locations that are secured consistent with their designated sensitivity level.	☐	☐	☐ ____	☐ ____	☐
2.2.18 Keys or other access devices are needed to enter the computer room and tape/media library.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming implementation and use of the required control.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.2.19 Secured area/perimeters (non-duty hours) are: (1) enclosed by slab-to-slab walls; (2) constructed of approved materials; (3) implemented by periodic inspection or other approved protection methods; and (4) any lesser type partition supplemented by UL approved electronic intrusion detection system. Unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded or locked with intrusion alarms. The space is cleaned during duty hours in the presence of a regularly assigned employee.	1. Review documentation confirming that secured area/perimeters have the required features. 2. Inspect a sample of audit data confirming that the space is cleaned during duty hours in the presence of a regularly assigned employee. 3. Inspect a sample of audit data confirming that the secured area/perimeters are consistently secured at the end of duty hours, and found secured when opened at the beginning of duty hours. 4. Confirm by inspection that the required electronic intrusion devices are in use.	☐	☐	☐ ____	☐ ____	☐
2.2.20 Allternate work site equipment controls are: (1) only business partner owned computers and software are used to process, access and store FTI; (2) specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the agency in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller, agency-owned equipment is locked in a storage cabinet or desk when not in use.	1. Review relevant policies and procedures for inclusion and directed use of the required process by personnel working from their homes or alternate worksites. 2. Inspect documentation confirming that the required controls are implemented and consistently used.	☐	☐	☐ ____	☐ ____	☐
2.2.21 Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	1. Review documentation designating specific individuals who are allowed access, and identifying the associated access control method used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review a sample of audit data confirming consistent use of the required access process.	☐	☐	☐ ____	☐ ____	☐
2.2.22 Management regularly reviews the list of persons with physical access to sensitive facilities.	1. Review a sample of audit data confirming periodic completion of the required reviews. 2. Review relevant policies and procedures for inclusion and directed use of the required process, and that they specify the review period.	☐	☐	☐ ____	☐ ____	☐
2.2.23 Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	1. Review audit data confirming consistent use of the required procedure. 2. Review documentation of the authentication procedure used for visitors, contractors, and maintenance personnel to confirm inclusion of the required controls.	☐	☐	☐ ____	☐ ____	☐
2.2.24 FTI in any form is protected during non-duty hours through a combination of secured or a locked perimeter, a secured area, or containerization.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used. 3. Review documentation establishing the protective methods and devices employed to protect FTI during non-duty hours. Confirm use of one or more of the following controls: (1) secured or locked perimeter; (2) secured area; or (3) containerization.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.2.25 All Restricted Areas used to protect FTI meet the criteria of IRS 1075 for secured area or security room, or provisions are made to store high security items in appropriate containers during non-duty hours.	If Restricted Areas are used to protect FTI, review documentation establishing that each meets the specific IRS requirements for either a "Secured Area" or a "Security Room", or that provisions have been made to store high security items in appropriate containers during non-duty hours.	☐	☐	☐	____	☐ ____ ☐
2.2.26 Unauthorized personnel are denied access to areas containing FTI during duty hours. Methods include use of restricted areas, security rooms, and locked doors.	1. If methods used to deny access to FTI by unauthorized personnel during duty hours do not include use of (IRS 1075 defined) Restricted Areas, Security Rooms, or Locked Rooms, then review documentation justifying use of alternative methods. 2. Review documentation establishing the methods employed to deny access to FTI from unauthorized personnel during duty hours.	☐	☐	☐	____	☐ ____ ☐
2.2.27 Procedures exist for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that the required process is consistently used.	☐	☐	☐	____	☐ ____ ☐
2.2.28 Security procedures are documented for bringing hardware and software into and out of the facility and for maintaining a record of those items.	Inspect documentation confirming that the required controls are implemented and consistently used.	☐	☐	☐	____	☐ ____ ☐
2.3 Access paths shall be identified.						
2.3.1 An analysis of the logical access paths is performed whenever changes to the system are made.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	____	☐ ____ ☐
2.4 Emergency and temporary access authorization shall be controlled.						
2.4.1 Access control implementation includes a procedure for emergency access and at least one of the following features: (a) context-based access; (b) role-based access; (c) user-based access.	1. Review documentation of the access control process to confirm inclusion of a procedure for emergency access. 2. Review documentation of the access control process to confirm inclusion of at least one of the required features.	☐	☐	☐	____	☐ ____ ☐
2.4.2 Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function and; (4) automatically terminated after a predetermined period.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that all four specified elements of the required process is consistently used.	☐	☐	☐	____	☐ ____ ☐
2.5 Resource classifications and related criteria shall be established.						
2.5.1 Computer System Security - All systems that process FTI meet the provisions of OMB Circular A-130, Appendix III and Treasury Directive Policy 71-10. All computers that process, store, or transmit FTI meet or exceed Controlled Access Protection (Level C2) as identified in IRS 1075, Sections 5.6 and 5.7, and Exhibit 6.	1. Inspect documentation identifying systems that process FTI. 2. Review documentation establishing that all computers in all specified systems meet C2 requirements in their implemented configuration. 3. Review documentation of the configuration management process used to assure that all C2 systems remain in C2 certified configurations.	☐	☐	☐	____	☐ ____ ☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.5.2 Classifications and criteria have been established and communicated to resource owners.	1. Review policies specifying classification categories and related criteria to be used by resource owners in classifying their resources according to the need for protective controls. 2. Inspect audit data confirming that the required policy has been communicated to resource owners.	☐	☐	☐ ____	☐ ____	☐
2.5.3 Only employees with "need-to-know" are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation establishing that existing safeguards provide the required protections.	☐	☐	☐ ____	☐ ____	☐
2.5.4 FTI is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that FTI is included. If FTI is recorded on removable storage devices or media with other data, it is protected as if it were entirely FTI. Computer access is restricted to authorized individuals.	1. Review FTI handling procedures for inclusion of the required processes. 2. For a sample of media and devices containing FTI, inspect to confirm use of the required labels.	☐	☐	☐ ____	☐ ____	☐
2.5.5 Every personnel position is designated with a sensitivity level.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample of personnel positions, inspect documentation establishing the associated sensitivity level.	☐	☐	☐ ____	☐ ____	☐
2.5.6 Documentation supports security and suitability standards that are being met by all personnel commensurate with their position sensitivity level, and that they are subject to personnel investigation requirements.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect a sample of audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
2.5.7 A security review cycle is established, so that all offices receiving FTI are reviewed within a three-year cycle.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.5.8 HCFA Business Partner office facilities processing FTI are subjected to a "self assessment" annually.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
2.5.9 Inspection reports, including self-assessment reports, and corrective actions are to be retained for a minimum of three years from the date of the inspection.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
2.5.10 FTI security systems are tested annually to assure that they are functioning correctly.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
2.5.11 FTI system design and test documentation are available including security mechanisms and implementation.	Inspect system design and test documentation for an explanation of C2 security mechanisms and how they are implemented.	☐	☐	☐ ____	☐ ____	☐
2.5.12 FTI system documentation contains the test policy, test plan, test procedures, retest procedures, and describes how and what mechanisms were tested, and the results.	Review the FTI system documentation for inclusion of the required C2 test documentation..	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.6 Actual or attempted unauthorized, unusual, or sensitive access shall be monitored.						
2.6.1 Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers.	1. Determine if system logs and events are compared against a database of known security violations and policies. 2. Verify use of automated detection software tools, both network and host-based.	☐	☐	☐	☐	☐
2.6.2 Security violations and activities, including failed logon attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software as required by FISCAM section 4.2. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
2.6.3 Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.	1. Review documentation of the controls used to enforce this requirement. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
2.6.4 Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including contractor employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.	1. Confirm by inspection that the required procedures exist. 2. By inspection confirm that supervisors have specified procedures.	☐	☐	☐	☐	☐
2.7 Owners of classified resources shall assign adequate classification to documentation and systems.						
2.7.1 Resources are classified based on risk assessments. Classifications are documented and approved by an appropriate senior official, and are periodically reviewed.	1. Review resource classification documentation and compare to risk assessments. 2. Inspect audit data confirming that the required approval and review processes are consistently used.	☐	☐	☐	☐	☐
2.7.2 Access to FTI is on a strictly "need-to-know" basis. Contractors evaluate the need for the FTI before the data is requested or disseminated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
2.8 Resource owners shall identify authorized users and the level of authorization.						
2.8.1 Security is notified immediately when system users are terminated or transferred.	1. Review relevant policies and procedures for inclusion and directed use of the required procedure. 2. Obtain a list of recently terminated employees from Personnel and determine whether system access was promptly terminated.	☐	☐	☐	☐	☐
2.8.2 All changes to security profiles by security managers are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming routine identification and investigation of unusual activity. 3. Review a selection of recent profile changes and activity logs.	☐	☐	☐	☐	☐
2.8.3 Security managers review access authorizations and discuss any questionable authorizations with resource owners.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.8.4 The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a selection of users with dial-up access, review authorization and justification.	☐	☐	☐ ____	☐ _____	☐
2.8.5 Owners periodically review access authorization listings and determine whether they remain appropriate.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ _____	☐
2.8.6 The supervisory mode of the on-line system is limited to workstations restricted for supervisory use.	Review documentation confirming use of the required restriction	☐	☐	☐ ____	☐ _____	☐
2.8.7 Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs. A separate authorization list is maintained that designates who is authorized access in emergencies and what limits are placed on their activities.	1. By inspection, confirm that authorization lists include the required information. 2. Inspect audit data confirming continuing maintenance of authorization lists and access controls for restricted areas.	☐	☐	☐ ____	☐ _____	☐
2.8.8 Warning banners advising safeguard requirements for FTI are used for computer screens.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. For a sample representing each type of computer operating system, and for standalone and each mode of network connection affecting banner display, observe that the warning banner on the sample computer is consistent with the documented procedure.	☐	☐	☐ ____	☐ _____	☐
2.8.9 Documented policies and procedures exist for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.	Review the appropriate documented policies and procedures for inclusion of the required rules.	☐	☐	☐ ____	☐ _____	☐
2.8.10 Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ _____	☐
2.9 Passwords, tokens, or other devices shall be used to identify and authenticate users.						
2.9.1 Attempts to log on with invalid passwords are limited to 3-4 attempts.	1. Review security software password parameters. 2. Review pertinent policies and procedures. 3. Observe the system directed action in response to four invalid access attempts, confirming that the action is consistent with the documented policy.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.9.2 Use of names or words as passwords is prohibited.	Review relevant policies for inclusion and directed use of the required prohibition.	☐	☐	☐	☐	☐
2.9.3 Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.	1. Interview a sample of users to confirm the required understanding and device possession. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
2.9.4 The use of passwords and access control measures are in place to identify who accessed protected information and limit that access to persons with a need to know.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review Access Authorization Lists to confirm designation of all users allowed access to each separate security partition within the system (e.g. each platform root logon, each application relating to a unique separation of duties boundary, and each network device that supports direct logon). 3. Review documentation describing audit systems implemented to record all accesses to protected information. 4. Review a sample personnel data confirming designated access permissions are consistent with each individual's position description. 5. Interview a sample of users to confirm use of individual logon accounts by each user, with no sharing. 6. Inspect a sample of access audit data supporting continuing use to the required process.	☐	☐	☐	☐	☐
2.9.5 When remotely accessing (from a location not directly connected to the LAN) databases containing FTI data: (1) Authentication is provided through ID and password encryption for use over public telephone lines. (2) Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location. (3) Standard access is provided through a toll-free number and through local telephone numbers to local data facilities. (4) Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provide data encryption as well.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of the specified controls for all dialup access to systems handling FTI. (Controls for packet switched network access are covered in other control techniques.) 3. Review audit data, including spot inspections, confirming that all the specified controls are applied to all dialup access. This includes review of all devices having potential access to FTI that are equipped with modems. 4. For a sample of access control devices, review the security configuration to confirm required use of the specified controls.	☐	☐	☐	☐	☐
2.9.6 Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), (d) telephone callback procedure, or (e) token.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation supporting implementation of the required controls. 3. Review a sample of audit data confirming continuing use of the required controls.	☐	☐	☐	☐	☐
2.9.7 Password files are encrypted.	1. View a sample dump of password files (e.g., hexadecimal printout). 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.9.8 Vendor-supplied passwords are replaced immediately.	1. For a sample of applications and network devices, attempt to log on using common vendor-supplied passwords. These default passwords are usually documented in the associated manuals. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.9.9 Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	1. Review pertinent policies and procedures. 2. Review documentation of such comparisons. 3. Interview security managers. 4. Make comparison using audit software.	☐	☐	☐ ____	☐ ____	☐
2.9.10 Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed periodically--every 30 to 90 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least six alphanumeric characters in length and prohibited from reuse for at least 6 generations.	1. Interview users. 2. Review security software password parameters. 3. Observe users keying in passwords. 4. Attempt to log on without a valid password. Make repeated attempts to guess passwords. 5. Assess procedures for generating and communicating passwords to users. 6. Review pertinent policies and procedures.	☐	☐	☐ ____	☐ ____	☐
2.9.11 Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords will be utilized where supported by existing operating systems.	1. Inspect a sample of workstations running each type of operating system in use to confirm that the required process is in use. 2. Review configuration documentation supported implementation of the required feature.	☐	☐	☐ ____	☐ ____	☐
2.9.12 Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.	Review documentation establishing that authorization control exists, and includes the required feature.	☐	☐	☐ ____	☐ ____	☐
2.10 Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure.						
2.10.1 Security software is used to restrict access. Access to security software is restricted to security administrators only.	1. Review documentation describing the security software in use for restriction of access to data files and software programs. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of security software parameters that limit access to the security software to security administrators.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.10.2 Security administration personnel set parameters of security software to provide access as authorized and restrict assess that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files and operating system files. Standardized naming conventions are used for resources.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Perform penetration testing by attempting to access and browse computer resources. (FISCAM 3.2.C) 3. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.(FISCAM 3.2.C) 4. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords.(FISCAM 3.2.C) 5. Review documentation describing the standardized naming conventions in use for resources.	☐	☐	☐ ____	☐ ____	☐
2.10.3 All executive software is stored so that it is available only to authorized executive software maintenance personnel.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation of controls used to restrict access to executive software to software maintenance personnel. 3. Review a sample of audit data confirming continuing use of the control.	☐	☐	☐ ____	☐ ____	☐
2.10.4 Updating of data is restricted to authorized employees.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List(s) identifying employees who are authorized to update data. 3. Inspect a sample of audit data confirming that the required process is consistently used 4. Review documentation of the control used to restrict of data updating to authorized employees.	☐	☐	☐ ____	☐ ____	☐
2.10.5 Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, uncatalog, scratch, and rename a file.	1. Review documentation of the process used to provide the specified control over routines that modify the status of a file. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect the Access Authorization List(s) for identification of personnel having the specified authorities.	☐	☐	☐ ____	☐ ____	☐
2.10.6 Inactive users accounts are monitored and removed when not needed.	1. Review a sample of audit data confirming continued operation of the required control. 2. Review documentation describing how the required control is implemented.	☐	☐	☐ ____	☐ ____	☐
2.11 Logical controls shall be implemented for databases and DBMS software.						
2.11.1 Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	1. Review security system parameters. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.11.2 Access and changes to DBMS software are controlled.	1. Review the controls protecting DBMS software. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.11.3 Use of DBMS utilities is limited.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the Access Authorization List for DBMS utilities to confirm access is limited to those personnel have an operational requirement for access.	☐	☐	☐ ____	☐ ____	☐
2.11.4 Database management systems (DBMS) and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails that allow monitoring of changes to the data dictionary and; (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	1. Interview database administrator. 2. Test controls by attempting access to restricted files. 3. Review pertinent policies and procedures.	☐	☐	☐ ____	☐ ____	☐
2.12 Sensitive material shall be protected.						
2.12.1 IRC 6103 authorizes the disclosure of FTI for use in statistical reports as long as it is released in a form that can not be associated with or otherwise identifies, directly or indirectly, a particular taxpayer. Authorized agencies adhere to the following or an IRS approved equivalent: (1) access to FTI is restricted to authorized personnel; (2) no statistical tabulation is released with cells containing fewer than three returns; (3) statistical tabulations prepared for geographic area below the state level are not released with cells containing data from fewer than ten returns; and (4) tabulations that would pertain to specifically identified taxpayers or that would tend to identify a particular taxpayer, either directly or indirectly, are not released.	1. Review a sample of audit data confirming consistent application of the required controls. 2. Interview personnel responsible for releasing statistical data and inspect samples to confirm compliance with the specified controls. 3. Review pertinent policies and procedures.	☐	☐	☐ ____	☐ ____	☐
2.12.2 Access to FTI is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
2.12.3 Workstations are prevented from obtaining access to sensitive applications programs and data not normally required at that workstation.	1. Review documentation designating the applications and data allowed to be obtained at each workstation. 2. Inspect to confirm that a person authorized access to applications and data exceeding restrictions on the sample workstation can not access those applications or data while logged on to that workstation. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation of controls used to enforce the requirement.	☐	☐	☐ ____	☐ ____	☐
2.12.4 Medicare data is not released to outside personnel unless their identity is verified.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
2. *Access Control*						
2.13 Suspicious access activity shall be investigated and appropriate action taken.						
2.13.1 Security managers investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.	☐	☐	☐	☐	☐
2.13.2 Violations are summarized and reported to senior management.	1. Interview senior management and personnel responsible for summarizing violations. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
2.13.3 Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
2.13.4 Any missing tape is accounted for by documenting search efforts and the initiator is notified of the loss.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
2.14 Owners shall determine disposition and sharing of data.						
2.14.1 Standard forms are used to document approval for archiving, deleting, and sharing data files.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect standard approval forms.	☐	☐	☐	☐	☐
2.14.2 Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	Examine documents authorizing file sharing and file sharing agreements.	☐	☐	☐	☐	☐
3. *System Software*						
3.1 Inappropriate or unusual activity shall be investigated and appropriate actions taken.						
3.1.1 Policy defines investigation of inappropriate or unusual activity and guidelines for appropriate actions to be taken.	Review system operational policies and guidelines.	☐	☐	☐	☐	☐
3.1.2 Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine when the last management review was conducted, and analyze their review regarding the intended functioning of software monitoring control techniques and controlling risk.	☐	☐	☐	☐	☐
3.1.3 The use of privileged system software and utilities is reviewed by technical management.	1. Interview technical management regarding their reviews of privileged system software and utilities usage. 2. Review documentation supporting technical management reviews. 3. Review documentation for system software utilities and verify that technical management has given use approvals.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
3. *System Software*						
3.1.4 Systems programmers' activities are monitored and reviewed.	1. Determine that system programmer supervisors are supervising and monitoring their staff. 2. Review documentation supporting the supervising and monitoring of systems programmers' activities.	☐	☐	☐ ____	☐ ____	☐
3.1.5 Systems support alarm features to provide immediate notification of predefined events.	1. Review security plan to determine use of audit logs and alarms set points. 2. Review audit logs.	☐	☐	☐ ____	☐ ____	☐
3.2 Policies and techniques shall be implemented for using and monitoring system utilities.						
3.2.1 Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.	1. Verify that the appropriate responsibilities have been defined. 2. Interview systems programmers regarding their responsibilities.	☐	☐	☐ ____	☐ ____	☐
3.2.2 Responsibilities for monitoring use are defined and understood by technical management.	1. Verify that the appropriate responsibilities are defined. 2. Interview technical management regarding their responsibilities.	☐	☐	☐ ____	☐ ____	☐
3.2.3 Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	1. Interview management and systems personnel. 2. Verify the existence and current version of the appropriate policies and procedures.	☐	☐	☐ ____	☐ ____	☐
3.2.4 The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	1. Determine whether logging occurs and what information is logged. 2. Review logs. 3. Using security software reports, determine who can access the logging files.	☐	☐	☐ ____	☐ ____	☐
3.3 Access authorizations shall be appropriately limited.						
3.3.1 Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.	1. Review pertinent policies and procedures. 2. Interview management and system personnel regarding access restrictions. 3. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 4. Attempt to access the operating system and other system software.	☐	☐	☐ ____	☐ ____	☐
3.3.2 Policies and procedures for restricting access to systems software exist and are up-to-date.	1. Interview management and systems personnel regarding access restrictions. 2. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. 3. Attempt to access the operating system and other system software. 4. Review pertinent policies and procedures.	☐	☐	☐ ____	☐ ____	☐
3.3.3 The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.	☐	☐	☐ ____	☐ ____	☐
3.3.4 Justification and management approval for access to systems software is documented and retained.	1. Interview system manager and security administrator. 2. Review appropriate documentation, and verify that it is retained.	☐	☐	☐ ____	☐ ____	☐
3.4 Installation of system software shall be documented and reviewed.						

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
3. *System Software*						
3.4.1 Installation of all system software is logged to establish an audit trail and reviewed by data center management.	1. Interview data center management about their role in reviewing system software installations. 2. Review a few recent system software installations and determine whether documentation shows that logging and management review occurred.	☐	☐	☐	☐	☐
3.4.2 Migration of tested and approved system software to production use is performed by an independent library control group.	Interview management, systems programmers, and library controls personnel, and determine who migrates approved system software to production libraries, and whether versions are removed from production libraries.	☐	☐	☐	☐	☐
3.4.3 Vendor-supplied system software is supported by the vendor.	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.	☐	☐	☐	☐	☐
3.4.4 Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	1. Interview management and systems programmers about scheduling and giving advance notices when system software is installed. 2. Review recent installations and determine whether scheduling and advance notification did occur. 3. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.	☐	☐	☐	☐	☐
3.4.5 Outdated versions of system software are removed from production libraries.	Review supporting documentation from a few system software migrations and the removal of outdated versions from production libraries.	☐	☐	☐	☐	☐
3.4.6 All system software is current and has current and complete documentation.	1. Review documentation and test whether recent changes are incorporated. 2. Interview management and system programmers about the currency of system software, and the currency and completeness of software documentation.	☐	☐	☐	☐	☐
3.5 System software changes shall be authorized, tested and approved before implementation.						
3.5.1 New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation.	1. Determine the procedures used to test and approve system software prior to its implementation. 2. Select a few recent systems software changes and review audit data confirming that the specified process was followed. 3. Review procedures used to control and approve emergency changes. 4. Select some emergency changes to system software and test whether the indicated procedures were in fact used.	☐	☐	☐	☐	☐
3.5.2 Policies and procedures exist and are up-to-date for identifying, selecting, installing and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	1. Interview management and systems personnel. 2. Verify that policies and procedures are current, and contain the required information.	☐	☐	☐	☐	☐
3.5.3 Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	1. Review procedures for identifying and documenting system software problems. 2. Interview management and systems programmers. 3. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
3. *System Software*						
3.5.4 New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	1. Determine what authorizations and documentation are required prior to initiating system software changes. 2. Select recent system software changes, and determine whether the authorization was obtained, and the change is supported by a change request document.	☐	☐	☐	☐	☐
3.5.5 Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.	Verify the existence of checkpoint and restart capabilities.	☐	☐	☐	☐	☐
3.5.6 Procedures exist for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.	1. Interview an independent IT supervisor who has previously reviewed changes. 2. Verify the existence of emergency change procedures. 3. Interview system managers.	☐	☐	☐	☐	☐
3.6 All access paths shall be identified and controls implemented to prevent or detect access for all paths.						
3.6.1 All accesses to system software files are logged by automated logging facilities.	Review sample accesses to system software files to confirm their being logged by automated logging facilities.	☐	☐	☐	☐	☐
3.6.2 Vendor-supplied default login IDs and passwords have been disabled.	1. Inquire whether disabling has occurred. 2. Test for default presence using vendor standard IDs and passwords.	☐	☐	☐	☐	☐
3.6.3 Remote access to the system master console is restricted. Physical and logical controls provide security over all workstations that are set up as master consoles.	1. Determine what terminals are set up as master consoles and what controls exist over them. 2. Test to determine if the master console can be accessed, or if other terminals can be used to mimic the master console and take control of the system.	☐	☐	☐	☐	☐
3.6.4 Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.	1. Obtain a list of all system software on test and production libraries used by the entity. 2. Verify that access control software restricts access to system software. 3. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated by the auditor, or at least in the presence of the auditor. 4. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.	☐	☐	☐	☐	☐
3.6.5 The operating system is configured to prevent circumvention of the security software and application controls.	1. Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods. 2. Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.	☐	☐	☐	☐	☐
3.6.6 The operating system's operational status and restart integrity is protected during and after shutdowns.	1. Interview the system manager. 2. Verify the protection of the operating system during and after shutdowns.	☐	☐	☐	☐	☐
4. *Segregation of Duties*						
4.1 Formal procedures shall guide personnel in performing their security duties.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
4. *Segregation of Duties*						
4.1.1 Detailed, written instructions exist and are followed for the performance of work.	1. Interview a sample of supervisors and subordinate personnel. 2. Confirm the existence of documented work instructions. 3. Observe the performance of work duties.	☐	☐	☐ ____	☐ ____	☐
4.1.2 Application run manuals provide instruction on operating specific applications.	Inspect run manuals for inclusion of the required instructions.	☐	☐	☐ ____	☐ ____	☐
4.1.3 Operators are prevented from overriding file labels or equipment error messages.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing how controls meet the specified requirement.	☐	☐	☐ ____	☐ ____	☐
4.1.4 Operator instruction manuals provide guidance on system operation. Documentation includes: (1) Security Features Users Guide and; (2) Trusted Facility Manual.	Determine that the required operator and security manuals exist, and that they provide the required documentation.	☐	☐	☐ ____	☐ ____	☐
4.1.5 The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing use of the specified approval process.	☐	☐	☐ ____	☐ ____	☐
4.1.6 Duties in critical control and financial functions are split. (e.g., establish special controls involving more than one person over blank and voided checks.)	1. Interview supervisors in the critical control and financial areas. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
4.2 Active supervision and review shall be provided for all personnel.						
4.2.1 All operator activities on the computer system are recorded on an automated history log.	Determine by review that an automated history log exists on each computer system, and that they record all operator activities.	☐	☐	☐ ____	☐ ____	☐
4.2.2 Personnel are provided adequate supervision and review, including each shift of computer operations.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming continuing supervision and review in accordance with the documented process.	☐	☐	☐ ____	☐ ____	☐
4.2.3 System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.	1. Interview supervisors and subordinate personnel to confirm continuing use of the required process. 2. Observe system startup. 3. Review audit data confirming that only authorized personnel are involved in the system startup operation. 4. Review audit data confirming that parameters set during IPL are consistently in accordance with documented procedures.	☐	☐	☐ ____	☐ ____	☐
4.2.4 Supervisors routinely review the history log and investigate any abnormalities.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review history log for signatures indicating supervisory review. 3. Inspect a sample of documentation of the supervisor's investigative process.	☐	☐	☐ ____	☐ ____	☐
4.3 Job descriptions shall be documented.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
4. *Segregation of Duties*						
4.3.1 Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	1. Review documentation establishing that existing documented job descriptions meet segregation of duty principles. 2. Inspect the effective dates of position descriptions to confirm that they are current. 3. Confirm by interview of the incumbents that documented job descriptions match actual current responsibilities and duties.	☐	☐	☐ ____	☐ ____	☐
4.3.2 Documented job descriptions include definitions of the technical knowledge, skills and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	1. Confirm by review that job descriptions are documented, and that they meet the specified criteria. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
4.4 Management shall review effectiveness of control techniques.						
4.4.1 Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
4.4.2 Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
4.5 Physical and logical access controls shall be established.						
4.5.1 Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	Review documentation establishing now physical and logical access controls accomplish the specified restriction.	☐	☐	☐ ____	☐ ____	☐
4.6 Employees shall understand their security duties and responsibilities.						
4.6.1 All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview employees to confirm that their job descriptions match their understanding of their duties and responsibilities, and that they carry out those responsibilities in accordance with their job descriptions.	☐	☐	☐ ____	☐ ____	☐
4.6.2 Local policy assigns senior management responsibility for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced and institutionalized within the organization.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
4.6.3 Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.	1. Review documented procedures identifying responsibilities for restricting access by job position in key operating and programming activities to confirm that these responsibilities are clearly defined. 2. Interview a sample of personnel identified as having the specified responsibilities to confirm that the responsibilities assigned are clearly understood and followed.	☐	☐	☐ ____	☐ ____	☐
4.7 Incompatible duties shall be identified and policies implemented to segregate these duties.						
4.7.1 Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Review approval controls.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
4. *Segregation of Duties*						
4.7.2 Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.	1. Review the required analyses for inclusion of the specified elements. 2. Confirm by review that the required analyses reflect current operations.	☐	☐	☐ ____	☐ ____	☐
4.7.3 Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.	1. Review documentation of process design establishing the specified separation of duties. 2. Confirm through interview, observation, and review of job descriptions for a sample of personnel, that these separation of duties requirements are met. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
4.7.4 Policies and procedures for segregating duties exist and are up-to-date.	Confirm through inspection that the required policies and procedures exist and are consistent with current operations.	☐	☐	☐ ____	☐ ____	☐
4.7.5 Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Confirm by review that documented operating procedures meet the required criteria.	☐	☐	☐ ____	☐ ____	☐
4.7.6 Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.	1. Review the agency organization chart showing IS functions and assigned personnel. 2. Interview selected personnel and determine whether functions are appropriately segregated. 3. Review relevant alternative or backup assignments and determine whether the proper segregation of duties is maintained. 4. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.	☐	☐	☐ ____	☐ ____	☐
5. *Service Continuity*						
5.1 Adequate environmental controls shall be implemented.						
5.1.1 Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.	1. Examine facility maintenance records for history of water damage. 2. Interview site managers for knowledge of potential pumping related hazards and familiarity with mitigation procedures. 3. Interview a sample of operations staff to confirm familiarity with mitigation procedures for potential plumbing related problems. 4. Observe the operation, location, maintenance, and access to the air cooling systems condensate drains. 5. Observe whether water can enter through the computer room ceiling or pipes are running through the facility, and that there are water detectors on the floor. 6. Review relevant procedures for inclusion mitigation measures for any potential plumbing related problems. 7. Review the current risk assessment to confirm investigation of the potential for plumbing related problems, and review risk mitigation plans for any such risks identified.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.1.2 Any behavior that may damage computer equipment is prohibited.	1. Review the risk assessment for identification of potentially hazardous employee activities. 2. Review relevant policies and procedures for inclusion and directed use of rules to prevent behavior considered potentially hazardous to IT equipment.	☐	☐	☐ ____	☐ _____	☐
5.1.3 Controls have been implemented to mitigate other disasters, such as floods, earthquakes and fire.	1. Review the risk assessment plan for consideration of the specified potential risks. 2. Review documentation of efforts to identify additional risks specific to the region, area, or facility. 3. Review documentation of risk mitigation planning covering all identified risks. 4. Review contingency plans, policies, and procedures supporting preparedness to mitigate identified risks.	☐	☐	☐ ____	☐ _____	☐
5.1.4 Environmental controls are periodically tested.	1. Review test policies. 2. Review documentation supporting recent tests of environmental controls.	☐	☐	☐ ____	☐ _____	☐
5.1.5 Redundancy exists in the air cooling system.	1. Review facility design documentation confirming air cooling system redundancy. 2. Review maintenance records confirming primary and redundancy systems are operational. 3. Observe demonstrations of operation of primary and redundant cooling systems. 4. Review policy and procedures relevant to operation and maintenance of primary and redundancy air cooling systems	☐	☐	☐ ____	☐ _____	☐
5.1.6 Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers and sprinkler systems).	1. Review facility drawings and other documentation documenting types and locations of the specified devices. 2. Review documentation of periodic inspections and maintenance of the specified devices and related systems to assure they are fully operational. 3. Review documentation supporting the qualifications of personnel inspecting and maintaining the specified devices and systems.	☐	☐	☐ ____	☐ _____	☐
5.1.7 A minimum degree of protection against fires is provided by installation of hand-held fire extinguishers suitable to the area (e.g., hand-held carbon dioxide extinguishers for electrical fires).	Verify by inspection that the specified fire extinguishers are installed, have current inspection certificates, and are readily accessible.	☐	☐	☐ ____	☐ _____	☐
5.1.8 Alarms can activate quenching systems with a delay feature that permits inspection of the possible trouble area and evacuation of the area before extinguishing agents are released.	Review documentation confirming that the specified delay system is installed and operational.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.1.9 An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.	1. Review facility documentation confirming installation of an uninterruptible power system (UPS). 2. Review design and test data supporting the capacity of the system to support the facility technical load long enough to allow shut down with lose of no more that transactions in progress at the time primary power is lost. 3. Review documentation supporting existence of periodic test, and preventive maintenance consistent with system specifications. 4. Review policies and procedures for orderly shut down of the system within the time allowed by the available UPS capacity. 5. Interview a sample of operations personnel for familiarity with the orderly shut down process and applicable documented procedures. 6. Review documentation supporting periodic test of the orderly shut down process.	☐	☐	☐ ____	☐ ____	☐
5.1.10 Management and the SSO have prearranged with the local fire department(s) the following safety control responsibilities for handling emergencies: (1) who will respond; (2) what is the best way to enter during and after working hours; (3) who will direct firemen to the fire; (4) where the data processing area is located; (5) what kind of area extinguishing system the computer room has; (6) where the controls for any smoke-exhaust systems are located and who should activate them and under what conditions; and (7) where the tape library is and what equipment/chemicals/procedures the firemen will use to prevent damage to the data contained on the tapes and disks.	1. Review documentation confirming that the specified arrangements are formally in place. 2. Review relevant policies and procedures for inclusion of the required processes and any interaction required to support the prearranged fire department activities. 3. Review documentation confirming that the specified arrangements are current.	☐	☐	☐ ____	☐ ____	☐
5.1.11 Alarms and fire protection are provided in the computer room, which include: (1) the placing of alarms or other protective devices on doors and windows to prevent unauthorized entry and, (2) fire detection equipment that includes alarm systems capable of indicating where the activated alarm is located. Water or other nontoxic systems are installed if area extinguishing systems are necessary.	1. Review documentation confirming that the required systems have been periodically inspected and tested to assure they are fully operational. 2. Review facility design documentation to verify that the appropriate alarms, and fire detection and protection equipment are installed.	☐	☐	☐ ____	☐ ____	☐
5.1.12 Alarm systems have a manually operated activating switch to provide alarm sounding capabilities if the automatic sounding system fails.	Review documentation verifying that the switch is installed, and is periodically tested to assure that it is operational.	☐	☐	☐ ____	☐ ____	☐
5.1.13 "Power-off" or "disconnect" controls are located where they are readily accessible to operating personnel, preferably at designated exit doors (inside the room). The controls are covered, but never locked, to prevent inadvertent deactivation. The controls allow shut off the ventilation system serving the operations area, as well as the power to all electrical equipment. Turning off the power does not put out the lights.	1. Interview a sample of operations personnel to confirm familiarity with the specified controls and associated procedures for their use. 2. Review documentation confirming that the specified controls are periodically inspected and tested to assure that they are fully operational. 3. Review policies and procedures covering use of the specified controls. 4. Review documentation verifying that the specified controls are installed, and include the required features.	☐	☐	☐ ____	☐ ____	☐

5.2 A Contingency Plan shall be documented in accordance with HCFA Contingency Plan Methodology.

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.2.1 The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.	1. Review the contingency plan to confirm inclusion of the specified provision. 2. Review documentation supporting timely availability of the backup personnel required by the contingency plan.	☐	☐	☐	☐	☐
5.2.2 User departments have developed adequate manual processing procedures for use until automated operations are restored.	1. Review documentation of analysis of the manual procedures confirming their coverage of critical operations, and assessing operational impact of manual operation. 2. Review the contingency plan for identification of the specified manual procedures. 3. Inspect the required manual procedures for consistency with the contingency plan. 4. Interview the relevant process managers to confirm familiarity with the required procedures.	☐	☐	☐	☐	☐
5.2.3 The Contingency Plan clearly assigns responsibilities for recovery.	Review the Contingency Plan to confirm clear identification of specific responsibilities for all elements of recovery.	☐	☐	☐	☐	☐
5.2.4 Contingency Plan consists of: (1) applications and data criticality analysis; (2) data backup and recovery; (3) disaster recovery plan; (4) emergency mode operation plan; and (5) testing and revisions.	Verify through inspection that the Contingency Plan includes the specified elements.	☐	☐	☐	☐	☐
5.2.5 Management and the SSO approve Contingency Plans.	1. Verify through inspection that all Contingency Plans have been approved by management and the SSO. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
5.2.6 Management and the SSO are able to show how the organization responds to specific disasters/disruptions to (1) protect lives, (2) limit damage , (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures and (5) minimize the impact on Medicare operations.	Determine through interview that system manager(s) and the SSO can explain how the organization covers each of the specified requirements through its response to specific disasters/disruptions.	☐	☐	☐	☐	☐
5.2.7 The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	Review the Contingency Plan emergency response procedures for inclusion of the required provision.	☐	☐	☐	☐	☐
5.2.8 Contingency Recovery Plans address the problems that a preplanned relocation entails, such as (1) time restraint complications, (2) operations degradation, (3) lost equipment replacement, (4) possible uncertainty as to availability of insurance funds and (5) limited choice of suitable alternative processing sites. Basics such as (1) temporary office space, (2) equipment, (3) replacement of key personnel lost as a result of the disaster/disruption, and (4) phones from which to conduct recovery operations are considered. Accurate inventories and floor plans are included in the HCFA Business Partner's Contingency Plan.	1. Verify through inspection that recovery plans identify and address basic requirements and problems expected to be encountered during execution of a preplanned relocation. 2. Verify through inspection that the HCFA Business Partner's Contingency Plan includes inventories and floor plans. 3. Verify through inspection, based on sampled data from the contingency plan, that the inventories and floor plans in that document are accurate. 4. Verify through inspection that recovery plans identify and address at least those basics and potential problems specified.	☐	☐	☐	☐	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.2.9 Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming that contingency plans have been reevaluated before any proposed major modifications were approved.	☐	☐	☐ ____	☐ ____	☐
5.2.10 Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	1. Review documentation supporting the contention that existing contingency plans protect storage media from improper modification in the event of system failure. 2. Review documentation describing use of installed security and backup capabilities to reduce the potential for data loss and/or modification during a system failure. 3. Review documentation describing use of software procedures to reduce the potential for data loss and/or modification during a system failure.	☐	☐	☐ ____	☐ ____	☐
5.2.11 The Contingency Plan identifies the HCFA Business Partner's critical interfaces that need to be established while recovering from a disaster.	Verify through inspection that the contingency plan identifies the specified interfaces.	☐	☐	☐ ____	☐ ____	☐
5.3 Critical data and operations shall be identified and prioritized.						
5.3.1 A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.	1. Verify by inspection that the required, prioritized list has been prepared. 2. Verify by inspection that the list is approved by senior management. 3. Review documentation supporting the contention that the list reflects current conditions. 4. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4 Data and program backup procedures shall be implemented.						
5.4.1 System and application documentation are maintained at the off-site storage location.	1. Review documentation supporting maintenance of the required off-site storage. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.2 Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent operation of the required rotation. 3. Verify by inspection the location of specific backup files. 4. Review documentation confirming successful periodic test of the ability to recover using backup files.	☐	☐	☐ ____	☐ ____	☐
5.4.3 The backup storage site is geographically removed from the primary site(s) and protected by environmental controls and physical access controls.	1. By inspection, verify that the backup storage facility is consistent with available documentation. 2. Review documentation confirming that the backup storage site meets the stated requirements.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.4.4 Contingency backup planning exists to assure the continuity of vital Medicare operations until full operational capability can be restored. This includes such things as (1) prioritizing operations; (2) identifying key personnel and how to reach them; (3) listing backup systems/records and where located; (4) stocking critical forms and supplies offsite; and (5) developing reliable sources for replacing equipment, supplies and forms on an emergency basis.	1. Review documentation confirming that contingency backup planning includes the specified elements. 2. Review documentation supporting the contention that backup planning assures continuity of vital Medicare operations.	☐	☐	☐ ____	☐ ____	☐
5.4.5 Host sites prepare and maintain backup plans covering Common Working File (CWF) operations as well as claims processing.	1. Review documentation confirming that the required backup plans are prepared and maintained. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.6 Contingency backup agreements are in writing and legally enforceable. Agreements state the following: (1) the kinds of disasters or disruptions covered; (2) what constitutes notification of intended use; (3) what space, equipment and processing hours will be available and for how many days; (4) whose staff will be used; (5) what security will be provided; and (6) what provisions are made for testing compatibility of equipment, software and data histories.	1. Review documentation supporting the contention that the backup agreements are legally enforceable. 2. Verify by inspection that backup agreements are in writing, and include the required elements.	☐	☐	☐ ____	☐ ____	☐
5.4.7 A backup copy of the Contractor's Security Profile is kept at secure off-site storage, preferably at the site where backup tapes and/or other backup facilities are located.	1. Verify by inspection that the backup copy is being kept as specified. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.8 The contractor keeps the backup copy of the security profile up-to-date, particularly for the Contingency Plan.	1. Review documentation confirming that the security profile is being kept up-to-date. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.9 Security and backup provisions are installed to reduce the potential for loss of data and/or improper modification of data during system failure.	Review documentation describing use of installed security and backup capabilities to reduce the potential for data loss and/or modification during a system failure.	☐	☐	☐ ____	☐ ____	☐
5.4.10 Backup copies of: (1) all claims data; (2) applications; (3) operating systems; and (4) utility software necessary for secure processing of Medicare claims offsite are updated and stored at the end of each production run.	1. Review audit data supporting consistent utilization of the specified process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.11 The old production program is retained as backup until new production results prove satisfactory when testing and implementing new programs.	1. Review audit data confirming consistent use of the required process. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.4.12 Procedures and mechanisms exist for the secured generation, storage, control and retrieval of backup files, data bases and computer programs, along with the ability to access or obtain backup equipment necessary for critical IT processes.	Verify by inspection that appropriate procedures and mechanisms exist.	☐	☐	☐ ____	☐ ____	☐
5.4.13 The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.	Review the Contingency Plan to verify that it contains the specified elements.	☐	☐	☐ ____	☐ ____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.5 Emergency processing priorities shall be established.						
5.5.1 Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming that the appropriate managers have approved the emergency processing priorities.	☐	☐	☐	☐	☐
5.6 Management and staff shall be trained to respond to emergencies.						
5.6.1 Data center staff have received training and understand their emergency roles and responsibilities.	1. Interview a sample of data center staff to confirm their understanding of their roles in emergency response procedures. 2. Review training records to confirm required training has been conducted, and is consistent with the current procedures.	☐	☐	☐	☐	☐
5.6.2 Emergency procedures are documented.	By inspection verify that documented emergency response procedures exist for all processes required by the emergency response plan.	☐	☐	☐	☐	☐
5.6.3 Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	Review training records to confirm that the required training has been delivered periodically.	☐	☐	☐	☐	☐
5.6.4 Emergency procedures are periodically tested.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming completion of the required testing. 3. Interview data center staff.	☐	☐	☐	☐	☐
5.7 The contingency plan shall be annually reviewed and tested.						
5.7.1 The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.	1. Review documentation of annual conduct of the required test. 2. Review documentation describing how the testing conditions simulate an emergency or disaster. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
5.7.2 Contingency Plans are reviewed whenever new operations are planned or new safeguards contemplated.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
5.7.3 Several copies of the current Contingency Plan are securely stored off-site at different locations, including homes of key staff members. It is reviewed once a year, reassessed and, if appropriate, revised to reflect changes in hardware, software and personnel.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data supporting consistent annual review, reassessment, and appropriate revision of the contingency plan as specified. 3. Review documentation confirming the required off-site distribution and storage.	☐	☐	☐	☐	☐
5.7.4 Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.7.5 The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documents establishing that the contingency plan and related agreements are adjusted as specified.	☐	☐	☐ ____	☐ ____	☐
5.8 Resources supporting critical operations shall be identified.						
5.8.1 Resources supporting critical operations are identified and documented. Types of resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect documents identifying resources supporting critical operations for inclusion of the specified resource types.	☐	☐	☐ ____	☐ ____	☐
5.9 There shall be effective hardware maintenance, problem management and change management to help prevent unexpected interruptions.						
5.9.1 Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ ____	☐
5.9.2 Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of the required logs. 3. Review documentation supporting conduct of the required analyses.	☐	☐	☐ ____	☐ ____	☐
5.9.3 Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations and testing.	☐	☐	☐ ____	☐ ____	☐
5.9.4 Goals are established by senior management for the availability of data processing and on-line services.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming establishment of the required goals.	☐	☐	☐ ____	☐ ____	☐
5.9.5 Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review samples of specific change management documentation for completed changes that support inclusion of the required scheduling considerations.	☐	☐	☐ ____	☐ ____	☐
5.9.6 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance, system downtime, and operational performance documentation for confirmation that operational performance has not been adversely affected by unscheduled maintenance.	☐	☐	☐ ____	☐ ____	☐
5.9.7 Records are maintained on the actual hardware performance in meeting service schedules.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required records.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.9.8 Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	1. Review documentation confirming availability of spare or backup hardware for support of applications designated as critical or sensitive. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review operations and maintenance documentation to confirm that levels of available backup or spare hardware have been sufficient to support system availability objectives.	☐	☐	☐ ____	☐ _____	☐
5.9.9 Hardware maintenance policies and procedures exist and are up-to-date.	1. Inspect maintenance policies and procedures. 2. Review documentation supporting the contention that the required policies and procedures are up-to-date.	☐	☐	☐ ____	☐ _____	☐
5.9.10 Regular and unscheduled hardware maintenance performed is documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review maintenance documentation for conformance with the documented procedures.	☐	☐	☐ ____	☐ _____	☐
5.9.11 Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	1. Inspect hardware maintenance schedules 2. Review documentation supporting the contention that the hardware maintenance schedule complies with vendor specifications. 3. Review maintenance records to confirm completion of hardware maintenance in accordance with the schedule. 4. Review documentation supporting the contention that the manner of performing maintenance minimizes the impact of maintenance on operations.	☐	☐	☐ ____	☐ _____	☐
5.10 Arrangements shall be made for alternate data processing and telecommunications facilities.						
5.10.1 Agreements have been established for a backup data center and other needed facilities that: (1) are in a state of readiness commensurate with the risks of interrupted operations; (2) have sufficient processing capacity and; (3) are available for use.	1. Review documentation supporting the contention that alternate facilities have sufficient processing capacity. 2. Inspect agreements established to confirm coverage of all identified alternate facilities. 3. Review documentation identifying facilities required for alternate data processing and telecommunications. 4. Review documentation supporting the contention that alternate facilities are in the required state of readiness. 5. Review documentation supporting the contention that alternate facilities are available for use.	☐	☐	☐ ____	☐ _____	☐
5.10.2 Alternate telecommunication services have been arranged.	Review documentation confirming the arrangement of alternate telecommunication services.	☐	☐	☐ ____	☐ _____	☐
5.10.3 Arrangements are planned for travel and lodging of necessary personnel, if needed.	Verify by inspection that the required arrangements have been planned.	☐	☐	☐ ____	☐ _____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
5. *Service Continuity*						
5.10.4 Planning includes an interim processing site in case backup processing has been severely limited in scope and the backup facility must be vacated before the damaged site can be restored or a new permanent site becomes operational.	Review documentation confirming that planning includes an interim processing site.	☐	☐	☐	☐	☐
5.10.5 Planning includes a recovery facility while backup operations are still underway and a separate recovery team, designated beforehand, to assure that both functions can be handled simultaneously.	1. Review documentation confirming that planning includes the required recovery facility. 2. Review documentation confirming that planning includes the required separate, predesignated recovery team.	☐	☐	☐	☐	☐
5.10.6 For cold sites, documented arrangements exist for rapid delivery of any necessary equipment.	Review documents arranging for the required equipment delivery to any cold sites.	☐	☐	☐	☐	☐
5.11 A contingency plan shall exist for any standalone computer workstations that specifies where backup data, software, and current operating procedures are stored.						
5.11.1 A Contingency Plan is available for each standalone computer workstation that specifies where backup data and software are stored. A single plan can cover more than one workstation.	1. Review the required contingency plan(s) to confirm inclusion of the specification of storage location(s) for backup data and software. 2. Review documentation confirming that the specified plan is available for each standalone workstation.	☐	☐	☐	☐	☐
5.11.2 Standalone computer workstation backup data, software and current operating procedures are stored in accordance with the Contingency Plan.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Through inspection for a sample of standalone workstations, establish that the specified storage criteria are met.	☐	☐	☐	☐	☐
5.12 Virus detection shall be performed.						
5.12.1 The HCFA Business Partner shall use virus identification, detection, protection, and elimination software.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the required software is installed and operational in accordance with documented policy.	☐	☐	☐	☐	☐
6. *Application Software Development and Change Control*						
6.1 Emergency changes to application software shall be promptly tested and approved.						
6.1.1 Emergency changes are documented and approved by the operations supervisor, formally reported to computer operations management for follow-up and approved after the fact by programming supervisors and user management.	1. Review the documented procedure required to process emergency changes. 2. Interview the operations supervisor, computer operations management, programming supervisors, and user management. 3. For a sample of emergency changes, observe the required documentation and approval steps.	☐	☐	☐	☐	☐
6.1.2 Emergency change procedures are documented.	Review the documentation of emergency change procedures.	☐	☐	☐	☐	☐
6.2 Use of public domain and personal software shall be restricted.						
6.2.1 Clear policies restricting the use of personal and public domain software have been developed and are enforced.	1. Review the required policies, and verify that they are enforced. 2. Interview the security administrator..	☐	☐	☐	☐	☐
6.3 Changes shall be controlled as programs progress through testing to final approval.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
6. *Application Software Development and Change Control*						
6.3.1 Test plans are documented and approved that define responsibilities for each party involved.	1. Interview the system manager. 2. Verify that test plans are documented and approved, and define the required responsibilities.	☐	☐	☐	____	☐	____	☐
6.3.2 Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions are applied.	For the software change request selected: (1) Compare test documentation with related test plans; (2) Analyze test failures to determine if they indicate ineffective software testing.	☐	☐	☐	____	☐	____	☐
6.3.3 A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.	1. Confirm the restrictions in the use of live data. 2. Interview the system manager. 3. Verify that test data will meet all processing criteria.	☐	☐	☐	____	☐	____	☐
6.3.4 Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.	1. Review documentation of all required departments for prompt and accurate updating. 2. Interview the system manager.	☐	☐	☐	____	☐	____	☐
6.3.5 Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.	1. Interview the software programming supervisor. 2. Review documented software changes to verify the tracing process.	☐	☐	☐	____	☐	____	☐
6.3.6 Program changes are moved into production only upon documented approval from users and system development management.	1. Interview user management. 2. Verify the documented approval of program changes before production implementation. 3. Interview system development management.	☐	☐	☐	____	☐	____	☐
6.3.7 Test results are reviewed and documented.	1. Verify that test results are reviewed and documented. 2. Interview the system manager.	☐	☐	☐	____	☐	____	☐
6.3.8 Changes to detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	1. Interview the programming supervisor. 2. Review documented changes to system specifications.	☐	☐	☐	____	☐	____	☐
6.3.9 Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).	1. Review test plan standards, and confirm that they follow all levels of testing and responsibilities. 2. Interview department supervisors to verify their compliance with test plan standards.	☐	☐	☐	____	☐	____	☐
6.3.10 Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	1. Determine when the last production program change was reviewed, and how often. 2. Interview data center management and/or the security administrator.	☐	☐	☐	____	☐	____	☐

Category / General Requirement / Control Technique	Protocol	Yes	No	Partial	Planned	N/A
6. *Application Software Development and Change Control*						
6.3.11 A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements.	1. Interview the system manager. 2. Confirm that the SDLC includes the three required elements.	☐	☐	☐ ____	☐ ____	☐
6.3.12 Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	1. Verify that the programming and software personnel have been trained in SDLC methodology, and that the training is current. 2. Interview the programming staff and the software staff.	☐	☐	☐ ____	☐ ____	☐
6.3.13 All important files, such as provider or history files, are designed so that no line item is lost. Every record is annotated with the ID of the person who updated it.	1. Interview the system manager. 2. Check a sample of important file records to ensure that the required ID is annotated.	☐	☐	☐ ____	☐ ____	☐
6.3.14 Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.	1. Interview the application system managers. 2. Review the documented policy to ensure that the required responsibilities are assigned.	☐	☐	☐ ____	☐ ____	☐
6.4 Access to program libraries shall be restricted.						
6.4.1 Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined.	☐	☐	☐ ____	☐ ____	☐
6.4.2 All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	Select a few program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tape.	☐	☐	☐ ____	☐ ____	☐
6.4.3 Production source code is maintained in a separate archive library.	1. Monitor libraries in use. 2. Verify that source code exists for a selection of production load modules by: (1) comparing compile dates; (2) recompiling the source modules; and (3) comparing the resulting module size to production load module size.	☐	☐	☐ ____	☐ ____	☐
6.4.4 Separate libraries are maintained for program development and maintenance, testing, and production programs.	1. Interview library control personnel. 2. Monitor libraries in use.	☐	☐	☐ ____	☐ ____	☐
6.5 Distribution and implementation of new or revised software shall be controlled.						
6.5.1 Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.	1. Examine procedures for distributing new software. 2. Check implementation orders for a sample of changes.	☐	☐	☐ ____	☐ ____	☐
6.5.2 Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.	☐	☐	☐ ____	☐ ____	☐
6.6 Programs shall be automatically labeled and inventoried.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
6. *Application Software Development and Change Control*						
6.6.1 Library management software is used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.	1. Interview personnel responsible for library control. 2. Examine a selection of programs maintained in the library and assess compliance with auditing procedures. 3. Review software change control policies and procedures.	☐	☐	☐ ____	☐ _____	☐
6.7 Authorizations for software modifications shall be documented and maintained.						
6.7.1 Change requests are approved by both system users and data processing staff.	1. Interview software development staff. 2. Identify recent software modifications and determine whether change request forms were used.	☐	☐	☐ ____	☐ _____	☐
6.7.2 Software change request forms are used to document requests and related approvals.	Examine a selection of software change request forms for approvals.	☐	☐	☐ ____	☐ _____	☐
6.8 Movement of programs and data among libraries shall be controlled.						
6.8.1 Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.	Examine related documentation to verify that procedures for authorizing movement among libraries were followed and before and after images were compared.	☐	☐	☐ ____	☐ _____	☐
6.8.2 A group independent of the user and programmers controls movement of programs and data among libraries.	Examine change control documentation to verify that procedures for authorizing movement among libraries were followed, and before and after images were compared.	☐	☐	☐ ____	☐ _____	☐
7. *Application System Authorization Controls*						
7.1 Source documents shall be controlled and shall require authorizing signatures.						
7.1.1 For batch application systems, a batch control sheet is prepared for a group of source documents and includes; date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.	1. Review the documented procedure for batch control sheet preparation. 2. Check a sample of batch control sheets to ensure the inclusion of the Control Technique elements.	☐	☐	☐ ____	☐ _____	☐
7.1.2 Access to blank documents is restricted to authorized personnel.	1. Interview a sample of personnel to confirm use of documented handling procedures. 2. Inspect blank document storage access controls for conformance to documented policy. 3. Review documented procedure containing authorized names and control of access.	☐	☐	☐ ____	☐ _____	☐
7.1.3 Source documents are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.	1. Inspect audit data confirming that the required process is consistently used. 2. Confirm that documents contain authorized signatures. 3. Review the documented procedure for recording and tracking of document numbers. 4. Review documentation identifying "key source documents".	☐	☐	☐ ____	☐ _____	☐
7.2 Master files shall be used to identify unauthorized transactions.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
7. *Application System Authorization Controls*						
7.2.1 Before transactions are processed, they are verified using master files of approved vendors, employees, etc., as appropriate for the application.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ _____	☐
7.2.2 Master files and program code that does the verification are protected from unauthorized modification.	1. Identify and observe the procedures employed that protect master files and program code. 2. Review the documented procedure covering the protection of master files and program code. 3. Inspect audit data confirming that the required process is consistently used. 4. Review documentation of software controls used in providing the required protection.	☐	☐	☐ ____	☐ _____	☐
7.3 Data entry workstations shall be secured and restricted to authorized users.						
7.3.1 All transactions are logged as entered, along with the workstation ID of the person entering the data.	1. Observe the processing of sample transactions, to ascertain that they are being logged correctly. 2. Review the documented procedure prescribing transaction logging.	☐	☐	☐ ____	☐ _____	☐
7.3.2 Each operator is required to use a unique password and identification code before being granted access to the system.	1. Interview a sample of management and data entry personnel to confirm consistent use of the documented procedure. Confirm that there is no sharing of passwords or identification codes. 2. Review documented login procedure. 3. Observe a sample of data entry login.	☐	☐	☐ ____	☐ _____	☐
7.3.3 Supervisors sign on to each workstation device or authorize workstation usage from a program file server, before an operator can sign on to begin work for the day.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented login procedure. 3. Observe supervisor login, prior to operator's sign on.	☐	☐	☐ ____	☐ _____	☐
7.3.4 When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Observe physical area during non-business hours.	☐	☐	☐ ____	☐ _____	☐
7.3.5 Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation use. 3. Observe workstation use.	☐	☐	☐ ____	☐ _____	☐
7.3.6 Each workstation automatically disconnects from the system when not used after a specific period of time.	1. Inspect audit data confirming that the required process is consistently used. 2. Review documented procedure for workstation configuration and use. 3. For a sample of workstation types, observe operation of the automatic disconnect process.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
7. *Application System Authorization Controls*						
7.3.7 Workstations with dial-up access are called back and generate a unique identifier code for computer verification before connection is completed.	1. Review documented dial-up procedure to confirm inclusion of the required features. 2. Observe a sample of dial-up connections involving each type of access controller.	☐	☐	☐ ____	☐ ____	☐
7.3.8 Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
7.3.9 Data entry workstations are located in physically secure environments.	1. Review System Security Plan. 2. Observe location of workstations.	☐	☐	☐ ____	☐ ____	☐
7.4 Users shall be limited to a set of authorized transactions.						
7.4.1 Authorization profiles for users limit what transaction data entry personnel can enter.	1. Review audit controls used to assure continued application of the required procedure. 2. Review documented procedure for data entry to confirm enforcement of the required limitation.	☐	☐	☐ ____	☐ ____	☐
7.4.2 Authorization profiles for workstations limit what transactions can be entered from a given workstation.	1. For a sample of each type of restricted workstation, observe attempted entry of a prohibited transaction by a logged on user who has the user permissions required to enter the transaction. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of configuration management assuring continued operation of the required controls. 4. Review documents designating transactions authorized from each workstation.	☐	☐	☐ ____	☐ ____	☐
7.5 Exceptions shall be reported to management for review and approval.						
7.5.1 Exception criteria and the related program code are protected from unauthorized modifications.	1. Review documentation of controls protecting exception criteria and associated program code. 2. Inspect documentation identifying personnel authorized to modify the specified software elements.	☐	☐	☐ ____	☐ ____	☐
7.5.2 Exceptions, based on parameters established by management, are reported for their review and approval.	1. Inspect audit data confirming that the required process is consistently used. 2. Determine that documentation of the required exists, and that it contains the required parameters that produce exceptions.	☐	☐	☐ ____	☐ ____	☐
7.6 Independent reviews of data shall occur before entering the application system.						
7.6.1 Supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.	1. Review documented procedure for pre-processing of data. 2. Interview a sample of supervisors and control unit personnel to confirm use of the process. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
7. *Application System Authorization Controls*						
7.6.2 Data control unit personnel monitor data entry and processing of source documents.	1. Interview management and data control unit personnel to confirm use of the process. 2. Review documented data entry and processing procedures. 3. Observe data entry and processing procedures.	☐	☐	☐ ____	☐ ____	☐
7.6.3 Data control unit personnel verify that source documents are properly prepared and authorized.	1. Inspect audit data confirming that the required process is consistently used. 2. Interview management and data control unit personnel to confirm use of the process. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Observe data control unit personnel performing the verification process.	☐	☐	☐ ____	☐ ____	☐
8. *Application System Completeness Controls*						
8.1 Computer sequence-checking shall be implemented.						
8.1.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review reports of missing or duplicate transactions. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
8.1.2 Sequence checking is used to identify missing or duplicate transactions.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
8.1.3 Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.	1. Observe the process that assigns unique sequence numbers to transactions without preassigned serial numbers. 2. Review the documented procedure that prescribes the assigning of unique sequence numbers. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
8.1.4 Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
8.2 Computer matching of transaction data shall be implemented.						
8.2.1 Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
8.2.2 Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.	1. Review the program specifications that describe the computer matching process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
8. *Application System Completeness Controls*						
8.2.3 For high-value, low volume items, individual transactions or source documents are compared with a detailed listing of items processed by the computer.	1. Review the documented procedure that describes the comparison process. 2. Inspect documentation identifying items designated as high-value, low volume. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
8.3 Reconciliations shall show the completeness of the data processed for the total cycle.						
8.3.1 Reconciliations are performed to determine the completeness of transactions processed, master files updated and outputs generated.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure describing the reconciliation process.	☐	☐	☐	☐	☐
8.4 Reconciliations shall show the completeness of data processed at points in the processing cycle.						
8.4.1 Record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.	1. Review the documented procedures for the data entry process. 2. Review a sample of data control reports for completeness of data entry.	☐	☐	☐	☐	☐
8.4.2 Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.	1. Interview the supervisory application programmer to determine that system controls are in place as prescribed by the application programs. 2. Inspect audit data confirming that the required process is consistently used. 3. Review the program specifications describing the reconciliation process for accurate data entry.	☐	☐	☐	☐	☐
8.4.3 Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	1. Review the documented procedures describing the reconciliation process for data entry. 2. Interview the supervisory application programmer to determine implementation of automatic reconciliation in completion of computer job runs. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
8.4.4 System interfaces require that the sending system's output control counts equal the receiving system's input counts.	1. Review the documented procedure describing the reconciliation process between systems. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
8.4.5 A data processing control group receives and reviews control total reports and determines the completeness of processing.	1. Review the documented procedure describing the data control group's function. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
8.5 Record counts and control totals shall be implemented on an IT System.						
8.5.1 For on-line or real time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness of data entry and processing.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedures for the data control and data entry process for inclusion of the required process.	☐	☐	☐	☐	☐
8.5.2 User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.	1. Inspect the process and documents for developing record counts and control totals to determine data entry completeness. 2. Review the documented procedures for the data control process. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐
9. *Application System Accuracy Controls*						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
9. *Application System Accuracy Controls*						
9.1 Erroneous data shall be reported back to the user departments for investigation and correction.						
9.1.1 Errors are corrected by the user originating the transaction.	1. Interview a sample of supervisors and subordinate personnel to confirm use of the documented procedure. 2. Inspect audit data confirming that the required process is consistently used. 3. Review the documented error correction procedure.	☐	☐	☐	☐	☐
9.1.2 Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	1. Interview a sample of supervisors and subordinate personnel to confirm that all specified reports and files have the required characteristics.. 2. Review sample error reports/files, and confirm that error messages contain the information specified in the Control Techniques. 3. Review the documented error processing procedure.	☐	☐	☐	☐	☐
9.1.3 All corrections are reviewed and approved by supervisors before the corrections are reentered.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented error correction procedure for inclusion of the required process. 3. Interview a sample of supervisors and subordinate personnel to confirm use of the required process.	☐	☐	☐	☐	☐
9.2 Automated entry devices shall be used to increase data accuracy.						
9.2.1 Effective use is made of automated entry devices to reduce the potential for data entry errors.	Review the documentation explaining how the specified objective is met.	☐	☐	☐	☐	☐
9.3 Rejected transactions shall be controlled with an automated error suspense file.						
9.3.1 Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure for processing reject data to confirm inclusion of the specified features.	☐	☐	☐	☐	☐
9.3.2 A control group is responsible for controlling and monitoring rejected transactions.	1. Review the documented procedure describing the control group's responsibilities and duties. 2. Interview a sample of the control group to confirm operational responsibilities match those documented.	☐	☐	☐	☐	☐
9.3.3 General controls effectively protect the suspense file from unauthorized access and modification.	Review the documentation describing how general controls provide the required protection of the suspense file.	☐	☐	☐	☐	☐
9.3.4 The suspense file is purged of transactions as they are corrected.	1. Review the documented procedure for the error correction process to confirm inclusion of the specified process. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
9. *Application System Accuracy Controls*						
9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.	1. Review the documented procedure for suspense file processing and transaction reconciliation. 2. Observe the suspense file process to confirm that the documented procedure is followed. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
9.3.6 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.	1. Review the documented suspense file procedure for inclusion of the specified processes. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
9.4 Source documents shall be designed to minimize errors.						
9.4.1 The source document is well-designed to aid the preparer and facilitate data entry . Transaction type and date field codes are preprinted on the source document.	1. Review documentation describing how source documents are "well designed to aid the preparer and facilitate data entry". 2. Inspect a sample of each type of source document to confirm inclusion of preprinted transaction type and date field codes.	☐	☐	☐ ____	☐ ____	☐
9.5 Overriding or bypassing data validation and editing shall be restricted.						
9.5.1 Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.	1. Review documentation establishing that the process for overriding /bypassing data validation and editing contains the required controls. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
9.6 Output production and distribution shall be controlled.						
9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.	1. Review the documented procedure assigning responsibility for output production and distribution. 2. Interview personnel assigned the specified responsibility to confirm application of the documented responsibility.	☐	☐	☐ ____	☐ ____	☐
9.6.2 The computer system automatically checks the output message before displaying, writing, and printing to make sure the output has not reached the wrong workstation device.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation confirming use of the required process. 3. Review documentation describing how the required control is implemented.	☐	☐	☐ ____	☐ ____	☐
9.6.3 The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the required schedule to confirm inclusion of the required elements. 3. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐ ____	☐ ____	☐
9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review sample printed reports to verify that it contains the elements required in the Control Technique.	☐	☐	☐ ____	☐ ____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
9. *Application System Accuracy Controls*						
9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review logs and check sample output, to verify that the required information is recorded.	☐	☐	☐	____	☐ ____ ☐
9.6.6 In the user department, outputs transmitted are summarized daily and printed for each workstation device and reviewed by supervisors.	1. Inspect audit data confirming that the required process is consistently used. 2. Review the documented procedure describing the output process and supervisory review.	☐	☐	☐	____	☐ ____ ☐
9.6.7 A control log of output product errors is maintained, including the corrective actions taken.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review the control log and confirm that it contains the required information.	☐	☐	☐	____	☐ ____ ☐
9.6.8 Each transmission of output to a user's workstation device is logged.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review a sample of the specified logs.	☐	☐	☐	____	☐ ____ ☐
9.6.9 Output from reruns is subjected to the same quality review as the original output.	1. Inspect audit data confirming that the required process is consistently used. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	____	☐ ____ ☐
9.7 Reports showing the results of processing shall be reviewed by users.						
9.7.1 Users review output reports for data accuracy, validity, and completeness. The reports include error reports, transaction reports, master record change reports, exception reports and control totals balance reports.	1. Review the documented procedure describing the review process and detailed report constituency. 2. Inspect audit data confirming that the required process is consistently used. 3. Review sample reports to confirm that they include the required elements specified in the Control Technique.	☐	☐	☐	____	☐ ____ ☐
9.8 Programmed validation and edit checks shall identify erroneous data.						
9.8.1 Program code for data validation and editing and associated tables or files are protected from unauthorized modifications.	1. Review the documented procedure describing the protection provided program code, files, or tables. 2. Observe the actions or procedures in place that protect program code, files, or tables.	☐	☐	☐	____	☐ ____ ☐
9.8.2 Programmed validation and edits include checks for: (1) reasonableness; (2) dependency; (3) existence; (4) mathematical accuracy; (5) range; (6) check digit; (7) document reconciliation; (8)) relationship or prior data matching.	1. Review the documented procedure describing programmed validation and edits for inclusion of the specifically required checks. 2. Inspect audit data confirming that the required process is consistently used.	☐	☐	☐	____	☐ ____ ☐
9.8.3 Validation and editing are performed at the computer workstation during data entry or are performed as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.	1. Review the documented procedure describing the specified validation and editing process. 2. Inspect audit data confirming that the required process is consistently used. 3. Observe the validation and edit process.	☐	☐	☐	____	☐ ____ ☐
9.9 When appropriate, preformatted computer workstation screens shall be used for data entry.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
9. *Application System Accuracy Controls*						
9.9.1 Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.	1. Review documented procedure specifying preformatted workstation screens, and describing screen prompts. 2. Observe a sample of workstation screens as personnel are processing data. 3. Interview the system administrator to confirm that the required feature is universally available..	☐	☐	☐ ____	☐ _____	☐
9.10 Tests shall be made for critical calculations.						
9.10.1 Program code and criteria for test of critical calculations are protected from unauthorized modifications.	1. Observe the measures in place that protect program code and testing criteria. 2. Review the documented procedure that describes the protection of program code and testing criteria.	☐	☐	☐ ____	☐ _____	☐
9.10.2 Programs perform limit and reasonableness checks on critical calculations.	Review documented analysis of program specifications that identifies critical calculations and confirms inclusion of the required checks.	☐	☐	☐ ____	☐ _____	☐
9.11 Key verification shall be used to increase the accuracy of significant data fields.						
9.11.1 The person assigned to rekey the data is sufficiently separated and independent from the original data entry person, so as to not negate the effectiveness of this process.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Interview the individual responsible for rekeying and the data entry supervisor.	☐	☐	☐ ____	☐ _____	☐
9.11.2 Significant fields are rekeyed to verify the accuracy of data entry.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming that the required process is consistently used. 3. Review documentation identifying fields that are to be rekeyed.	☐	☐	☐ ____	☐ _____	☐
10. *Network*						
10.1 LAN/Computer Room Access Controls shall be in place.						
10.1.1 An access list of personnel authorized to access a data center to process sensitive data is controlled.	1. By inspection confirm existence of the required access list(s) for both physical and electronic access to each data center. 2. Review audit data confirming control of access lists in accordance with documented procedures. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐ ____	☐ _____	☐
10.1.2 Physical access to enclosures housing network equipment is restricted.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Select a sample of network equipment locations representative of the range of types of physical locations within each facility. For these sample equipments, confirm that access to them is restricted in accordance with the documented procedure.	☐	☐	☐ ____	☐ _____	☐
10.2 Network system security shall be monitored for deficiencies.						

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
10. *Network*						
10.2.1 Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation identifying devices selected to provide the specified logging function. 3. By inspection of a sample of the logs, confirm that they include network and system activity.	☐	☐	☐	☐	☐
10.2.2 Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network.	1. Confirm by inspection that virus-scanning software is installed. 2. Confirm by inspection that virus-scanning software is installed. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation identifying designated critical network entry points.	☐	☐	☐	☐	☐
10.3 Facsimile and E-mail shall be controlled.						
10.3.1 All Facsimile transmissions of sensitive information, including FTI, are encrypted.	1. Inspect a sample of facsimile transmission system configurations to confirm that controls are in place in accordance with the documented procedure. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation establishing controls to assure that all facsimile transmissions of sensitive information are encrypted.	☐	☐	☐	☐	☐
10.3.2 Telephone numbers of the facsimile machines receiving information are verified before transmitting data.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect logs confirming conduct of the required verification.	☐	☐	☐	☐	☐
10.3.3 Facsimile machines receiving sensitive data are in a secured area.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. By inspection confirm that each facsimile machine is in a secured location.	☐	☐	☐	☐	☐
10.3.4 Procedures exist to enforce E-mail security, privacy, and message integrity.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
10.3.5 Policy exists identifying appropriate use of the E-mail systems by employees.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
10.3.6 Policy and procedures exist to assure that facsimile machines in common areas are only used for data at Sensitivity Level 1.	Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
10.3.7 Security policy exists and audit reviews include checks, to assure that system administrators and others with special system level access privileges are prohibited from reading the electronic mail messages of others unless authorized on a case by case basis by appropriate management officials.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect the audit process for operation in accordance with the documented process.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
10. *Network*						
10.3.8 Contact is made to the receiving party before sending the facsimile transmission.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review logs to confirm that the required contact has been made.	☐	☐	☐	☐	☐
10.4 Cryptographic tools shall be controlled.						
10.4.1 FTI data being electronically transmitted must be protected. Two acceptable methods for transmitting FTI over telecommunications devices: (1) encryption and (2) guided media.	1. Confirm by inspection that documented controls are in place and operational. 2. Review relevant policies and procedures for inclusion and directed use of the required process. 3. Review documentation of controls used to assure protection of electronically transmitted FTI. 4. Review documentation establishing approval of the protection methods utilized.	☐	☐	☐	☐	☐
10.4.2 Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	1. Review documentation establishing that the required protection has been implemented. 2. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
10.5 Adequate Network password policies shall be implemented.						
10.5.1 Reusable passwords are encrypted in transmission and storage.	1. Review documentation of controls used to assure that all systems remain configured to use the specified feature. 2. Review documentation explaining how this feature is implemented on each network and local computing environment. 3. Review relevant policies and procedures for inclusion and directed use of the required process.	☐	☐	☐	☐	☐
10.6 Internet Security Policies shall be made available.						
10.6.1 HCFA Business Partner's Internet connections must be in accordance with the HCFA Internet Security Policy. When a determination for Internet use has been made, it shall include at a minimum of Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems (HCFA Internet Security Policy November 24, 1998).	1. Review documentation describing protections to assure that all virtual private network connections using the Internet are encrypted in accordance with the requirement. 2. Review documentation describing protections to assure that the only interconnections allowed between the Internet and networks carrying sensitive information are the specified virtual private network connections. 3. Review relevant policies and procedures for inclusion and directed use of the required process. 4. Review documentation describing the approved authentication process used to allow establishment of the virtual private network connection to a local network or other system carrying sensitive information.	☐	☐	☐	☐	☐
10.7 Configuration Control Policy shall be documented and available.						
10.7.1 Purchased software is used in accordance with contract agreements and copyright laws	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing audit and inventory processes and tools in use to detect improper use of software.	☐	☐	☐	☐	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
10. *Network*						
10.7.2 Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Confirm by inspection that the specified controls are in place and operating in accordance with the documented procedure. 3. Review documentation describing the software tracking system implemented to provide the specified controls.	☐	☐	☐ ____	☐ _____	☐
10.7.3 A change-control mechanism that maintains control of changes to hardware, software, and security mechanisms is implemented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review audit data confirming use of the documented change-control mechanism. 3. Review documentation describing the change-control mechanism that is implemented to provide the specified controls.. 4. For a sample of hardware, software, and security mechanism, determine by inspection that the configuration of the sample item matches the documented baseline configuration for the item. 5. Compare sampled data, such as device type, serial number, and software version, from the current configuration management baseline system description with corresponding hardware, software, and security mechanism implementation to confirm precise match.	☐	☐	☐ ____	☐ _____	☐
10.8 Logical Network Access Controls shall be in place.						
10.8.1 Any connection to the internet, or other external networks or systems, occurs through a gateway/firewall.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing controls implemented to insure compliance with this requirement.	☐	☐	☐ ____	☐ _____	☐
10.8.2 Strong authentication is used to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; (3) grant access to the functions of critical network devices; (4) procedures for the above are documented.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation describing implementation of all required authentication functions. 3. Review documentation describing the user certification and revocation processes used to support the required strong authentication.	☐	☐	☐ ____	☐ _____	☐
10.8.3 The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.	1. Review relevant policies and procedures for inclusion and directed use of the required process and specification of the warning message(s) to be used. 2. View the required warning message displayed on the opening screen seen by system users each type of server, workstation, and terminal used in the system. 3. For a sample, including each type of network device supporting the feature, view the required warning message displayed on the opening screen seen by anyone attempting to directly access the device from the network or console.	☐	☐	☐ ____	☐ _____	☐

Category General Requirement Control Technique	Protocol	Yes	No	Partial	Planned	N/A
10. *Network*						
10.8.4 Dial-in phone numbers are not published and are periodically changed.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Review documentation of the process used to implement the required controls. 3. Inspect audit data confirming continuing use of the required process.	☐	☐	☐	☐	☐
10.9 Vulnerabilities to physical and cyber attacks shall be assessed.						
10.9.1 A plan is in place to assess the risks to the network.	Review the required plan and approved implementing instructions.	☐	☐	☐	☐	☐
10.9.2 A plan is developed for eliminating significant vulnerabilities.	1. Review the required plan. 2. Review documentation establishing that the required plan eliminates all significant vulnerabilities.	☐	☐	☐	☐	☐
10.9.3 A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the HCFA Business Partner IS systems.	Review the required plan to confirm that it includes the specified features.	☐	☐	☐	☐	☐
10.9.4 Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	1. Review relevant policies and procedures for inclusion and directed use of the required process. 2. Inspect audit data confirming conduct of the required assessments at least annually.	☐	☐	☐	☐	☐
10.10 Logical controls shall be implemented over telecommunications access.						
10.10.1 Communication software has been implemented to verify workstation identifications in order to restrict access through specific workstations: (1) verify IDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity logs; (7) restrict access to table that define network options, resources, and operator profiles; (8) allow only authorized users to shutdown network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.	1. Review documentation confirming implementation of communications software having all of the required features. 2. Review audit data confirming continuing operation of all specified features of the required software.	☐	☐	☐	☐	☐